NATIONAL DEFENCE UNIVERSITY (KENYA)

NATIONAL DEFENCE COLLEGE (KAREN)

RESEARCH THESIS

CYBERCRIME AND IMPLICATIONS ON ECONOMIC SECURITY: THE CASE OF KENYA

BY

ISSA CHOCHOTE SAIDI

SUPERVISORS

Col. Dr. James Kimuyu

Col. (Rtd). Dr. Steve Handa

September 2024

DECLARATION

I hereby declare that this research thesis is entirely my own original composition, and it has not been presented in any other University.

Signature..... Date.....

Issa Chochote Saidi

ND. 601/0057/2023

This research thesis has been submitted for examination with my approval as the University Supervisor.

Signature..... Date.....

Col (Dr). James J. Kimuyu, 'psc' (K)

National Defence University, Kenya

Signature..... Date.....

Col (Rtd) Dr Steve Handa

National Defence University, Kenya

DEDICATION

A special feeling of gratitude and dedication goes to my family, friends and relatives. May Allah bless them all.

ACKNOWLEDGEMENT

I extend my appreciation to everyone who played a role in the accomplishment of this research thesis. I am especially grateful to Dr. James Kimuyu and Dr. Steve Handa, my supervisors, for their invaluable guidance throughout this research endeavor. Additionally, I am grateful to the National Defence University and the National Defence College for their support in providing the necessary resources and academic environment for this study. My appreciation is further extended to also the library staff, the respondents, my fellow colleagues, who in one way or another made a contribution to this study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

ATM	Automatic Teller Machine
CSR	Corporate Social Responsibility
DDOS	Distribution Denial of Service
DIME	Diplomatic Information Military Economic
DRC	Democratic Republic of Congo
GoK	Government of Kenya
ICT	Information Communication Technology
IR	International Relations
IT	Information Technology
ITU	International Telecommunication Unit
KA	Kenya Army
KAF	Kenya Air Force
KDF	Kenya Defence Forces
KE-CIRT/C	Kenya National Computer Incident Response Team Coordination Centre
KN	Kenya Navy
KRA	Kenya Revenue Authority
LAN	Local Area Network
LOIC	Low Orbit Ion Canon
MoD	Ministry of Defence
NACOSTI	National Commission for Science Technology and Innovation
NDA	Non-Disclosure Agreement
NDC	National Defence College
NDU	National Defence University
ODPP	Office of Director of Public Prosecution
RDF	Rwandan Defence Forces
SPSS	Statistical Package for Social Science

SSA	Sub Saharan Africa
UK	United Kingdom
UN	United Nations
UNO	United Nations Office
US	United States

OPERATIONALIZATION OF TERMS

Computer in this research refers to a device that takes information usually in the form of digitalized data and that is ideally manipulated based on a program, software and also a system that automatically takes a set of instructions on how the data is stored, processed and retrieved (Breamner, 2017).

Cyber is understood as a prefix indicating anything related to computers, computer networks, or virtual reality. It's commonly used to form compound words like "cyberspace" and is also associated with futuristic visions (Kenya Cyber Security Report, 2014).

Cybercrime in this study generally refers to the use of computer or cyber technology in a wide range of criminal activities some of which include use of technology to commit fraud, data breaches, computer viruses, computer scams, identity theft and many other malicious cats(Kenya Cyber security Report, 2014).

Development is a process that seeks to improve the quality of life and create opportunities for individuals and societies to reach their full potential. In this study it is understood as an approach that balances economic growth with social progress, environmental sustainability, and cultural vitality (Ahorro, 2008).

Information Technology in this study refers to the utilization of computer systems that enable one to solve, process, manage, store and exchange information. The information is designed to encourage the use of technology with the aim of solving day-to-day challenges (Okongo, 2021).

Malware broadly in this study denotes to the application of a computer virus or malware for criminal purposes. Some of these malwares attacks are designed for stealing confidential data, because data damage, carry out criminal acts and also seek ransom (GoK, 2014).

National economic development is the country's capacity to raise its residents' living standards of the main citizens. Providing individuals with basic livelihood requirements and supplying them with employment opportunities, better homes, and businesses can achieve it (Ahorro, 2008).

Operating system is defined as a program that manages a computer system, via the central processing unit, computer memory, file storage and also particularly the allocation of those resources among other programs (Kenya Cyber-Security Report, 2014).

Phishing in this research refers to some form of technological campaign through the use of spam emails and or other forms of communications with the intent of deceiving, misleading and or pretenses that undermine cyber security (Sayigh, 2023).

Soft Power in the context of International Relations (IR) as used in this study denotes the ability to persuade or co-opt states, organizations and individuals, through appeal and attraction between Kenya and other countries (Okongo, 2021).

Technology in the context of this research refers to the application of conceptual knowledge with the intention of solving practical goals, especially in a reproducible way; and therefore technology refers to products resulting from these efforts (Sayigh, 2023).

ABSTRACT

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

Keywords: Cybersecurity, economic security, national security, internet, Kenya.

CHAPTER ONE

INTRODUCTION

1.0 Introduction

This chapter provides an overview of the primary research theme explored in the study. It begins with a detailed statement of the research problem, outlining the central issue under investigation, which is cybercrime and its iumplications on economic security in Kenya. The chapter then presents the rationale behind the study, explaining why this topic is of critical importance and how understanding it can contribute to enhancing Kenya's cybersecurity posture. Following this, the chapter specifies the research objectives, which are designed to address the identified problem and achieve the study's goals. These objectives include assessing the effects of cybercrime on Kenya's economic stability, examining the elements of cybercrime that threaten economic security, and evaluating the effectiveness of current response mechanisms.

The chapter also outlines the scope of the study, detailing the boundaries and limitations of the research. This includes the specific aspects of cybercrime and economic security that will be examined, as well as any constraints that may affect the study's findings. The chapter then finally describes the methodology adopted for the research. This includes the theoretical framework guiding the study, the research design and methods used for data collection and analysis, and the rationale for choosing these methods. The methodology section ensures that the approach taken is rigorous and appropriate for addressing the research problem and achieving the study's objectives

1.1 Background of the Study

Countries around the world are increasingly recognizing the urgent need to address cybercrime to safeguard their economic stability. For example, the United States has implemented a multi-layered approach to combat cyber threats through the establishment of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) (U.S. Department of Homeland Security, n.d.). This agency works to protect critical infrastructure by offering resources and guidance to both public and private sectors. Additionally, the U.S. employs a proactive stance by engaging in international collaborations and intelligence-sharing initiatives to address global cyber threats (U.S. Cybersecurity and Infrastructure Security Agency, 2023). The focus is on improving the resilience of digital systems through advanced threat detection technologies, regular security audits, and comprehensive response strategies to mitigate potential economic damage (U.S. Cybersecurity and Infrastructure Security Agency, 2023).

In Europe, the General Data Protection Regulation (GDPR) represents a significant effort by the European Union to enhance cybersecurity and protect economic interests (European Commission, 2020). The GDPR imposes stringent data protection requirements on organizations, ensuring that they adopt robust cybersecurity measures to safeguard personal data. Countries within the EU also participate in the European Union Agency for Cybersecurity (ENISA), which provides expert guidance, supports the implementation of cybersecurity strategies, and fosters cross-border cooperation (European Union Agency for Cybersecurity, 2021). These initiatives are designed to reduce the risk of cyber-attacks and their potential economic impact by promoting best practices in data protection and incident response (European Union Agency for Cybersecurity, 2021).

In Asia, Singapore has emerged as a leader in cybersecurity through its comprehensive national strategy, the Singapore Cybersecurity Strategy (Cyber Security Agency of Singapore, 2016). This strategy emphasizes a holistic approach to cyber defense, including the development of advanced cyber capabilities, robust public-private partnerships, and extensive public awareness campaigns (Cyber Security Agency of Singapore, 2016). Singapore's approach involves the creation of a dedicated national cybersecurity agency, the Cyber Security Agency of Singapore (CSA), which oversees the implementation of cybersecurity measures across various sectors (Cyber Security Agency of Singapore, 2016). By focusing on building a resilient cyber infrastructure, promoting cybersecurity education, and fostering collaboration with international partners, Singapore aims to mitigate the economic risks associated with cybercrime and enhance its overall cyber resilience (Cyber Security Agency of Singapore, 2016).

Cybercrime poses a significant threat to economic security in Africa and Kenya specifically through various avenues, including financial losses, disruption of critical infrastructure, and erosion of trust in digital systems. At present, the Africa continent is experiencing a surge in various aspects, including population, economic development, and global influence. Presently, the continent is home to 1.21 billion people, a significant increase from 800 million in 2000, with a median age of 19.5 years, making it the youngest population globally (Statisca, 2024). This youthfulness brings diversity, as the population seeks productive employment, social engagement, freedom of expression, and enhanced global connectivity. Despite challenges such as the impact of declining global commodity prices on African economies, nearly every African nation is positioned for growth in the coming years.

These changing dynamics in Africa have led to a rise in the adoption of technology, marked by the exponential growth in mobile device ownership, increased use of social media, and the rapid emergence of the Internet of Things (IoT). Conservative estimates suggest that Africa is on the verge of significant progress, contributing to global growth. Alongside this economic expansion, the e-commerce sector has experienced rapid rise to the point that it is expected to reach an estimated $75 billion USD by 2025 (Mitchell, 2022). However, as prosperity and digitization has increased, new risks and vulnerabilities have also emerged that are potentially hindering progress. One major concern is the global surge in cybercrime. As Africa's economy transitions to the online realm, citizens, their computer systems, and the continent's information technology (IT) infrastructure become attractive targets for an increasingly sophisticated group of cybercriminals. Latest research shows that over the past decade, Africa's international internet bandwidth experienced a tenfold increase to 12 terabits per second (Tbps). The International Finance Corporation (IFC), a division of the World Bank, anticipates a substantial 11% surge in internet users in Africa over the next decade, accounting for 16% of the global total. Additionally, the transition from 3G to 4G is underway, with 4G expected to surpass 28% of the continent's mobile phone connections by 2025, up from 12% in 2020, according to GSMA, the lobby organization for mobile communication companies. Research conducted by the IFC and Google suggests that Africa's digital economy is poised to contribute $180 billion to the overall economy by 2025, reaching $712 billion by 2050 (Sukumar and Amoozad, 2023).

Research further shows that at the end of 2020, mobile service subscriptions in sub-Saharan Africa had already reached 495 million, representing 46% of the region's population and marking a nearly 20 million increase from 2019, according to GSMA, a telecommunications association. Simultaneously, 303 million individuals in the region had access to mobile internet. The tally of

registered mobile money wallets in Africa surpassed 621 million in 2021, reflecting a 17% rise from 2020. The value of mobile money transactions in Africa surged by 39% to reach $701.4 billion in 2021 (Mitchell, 2022).

1.2 Statement of the Problem

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

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

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

1.3 Research Objectives

1.3.1 The general objective

The primary objective of this research is to investigate how cyber-crime poses a risk to economic stability in Kenya.

1.3.2 The specific objectives

The study was guided by the following specific objectives

i. To examine elements of cybercrime posing a threat to the economic security of Kenya.

ii. To assess the effects of cybercrime on Kenya’s economic stability.

iii. To evaluate response mechanism to cybercrime as a threat to economic security in Kenya.

1.4 Research Questions

The study was guided by the following research question:

i. How do elements of cybercrime pose a threat to Kenya's economic security?

ii. What are the effects of cybercrime on Kenya's economic stability?
iii. How effective are the response mechanisms to cybercrime in addressing the threat to Kenya's economic security?

1.5 Justification of the study

Cybercrime poses a significant threat to Kenya's economy. It can result in financial losses for businesses, government institutions, and individuals through activities such as hacking, fraud, identity theft, and extortion. These financial losses can have a direct impact on the country's GDP and overall economic stability. Therefore, this study is useful in generating further ideas on how Kenya can cushion safeguard itself from the risks of cybercrime during its engagement in the digital world.

1.5.1 Academic justification

This study aims to evaluate academic literature on emerging trends and patterns of cybercrime, which could be useful to scholars and academicians dealing with the subject matters. Given the ever-expanding number of cyber-technological threats online today, the fluidity and sophistication of cybercrime, and even with the efforts by the various agencies including cybercrime experts, cybercrime is more likely to increase rather than decrease.

1.5.2 Sensitization justification

The idea of cyber-technology is diverse, and therefore cybercrime can fuel elements seeking to publicize dangerous political views, extremist ideas, criminal organizations seeking financial gain, terrorist groups seeking to inflict economic or political damage, to state-sponsored intelligence and security organizations. Cyber-crime is relatively building in its evolution and has been associated with individuals, terrorist groups and state actors, could escalate into a *cyber-war,* thus this study

aims sensitize the general public on cyber-crime as threat to economic security in Africa particularly in Kenya.

1.6 Significance of the study

Cyber security challenges in developing states seem to have a common approach and proposed frameworks, unfortunately these developing states have shortcoming and this study will help develop strategies and inform how African states could better approach their cyber security problems, such as cybercrime (Sayigh, 2023). Hence, in addressing cybercrime threat to economic security in Kenya, this study argues that developing states have been trying to imitate what is being done by developed world, which this research found is not a good approach. The country needs to innovate and come up with its solutions that will best deal with cybercrime as threat to economic security in Kenya.

1.7 Assumptions of the study

Kenya has gone ahead to develop strategies to respond to the rising cyber security threats by adapting to internationally recognized standards (Gagliardone, 2014). This section notes that recognizing the importance of ICT in economic development, Kenya has chosen to seek partnerships with actors in the digital world to develop a strategy based on their experiences on the risks. With the backing of the International Telecommunications Unit (ITU), the government has established a body called Kenya National Computer Incident Response Team Coordination Centre (KE-CIRT/CC) to offer technical services in the management of cyber security.

1.8 Scope and Limitations of the Study

This study was undertaken in Nairobi County, with a focus on the most affected constituencies within the city. In addition, the study has a restricted timeline of between 2014 and 2024. It is important to note that this research experienced some difficulties in securing the input of subject matter experts (respondents), owing to the sensitive and technical nature of their work. Therefore, in order to mitigate this, the researcher strived to identify the research prospects in advance, possible through snow balling, plus effectively applied proper research technique in the study and adhered to guidance from various institutions.

1.9 Chapter Summary

Chapter one of this study has provided an examination of existing research, including an exploration of current theories, empirical studies, and the theoretical framework relevant to the research objectives. The chapter also outlined the scope of the study, detailing the boundaries and limitations of the research. This included the specific aspects of cybercrime and economic security that were examined, as well as any constraints that might have affected the study's findings. The chapter then described the methodology adopted for the research. This included the theoretical framework that guided the study, the research design, the methods used for data collection and analysis, and the rationale for choosing these methods. The methodology section ensured that the approach taken was rigorous and appropriate for addressing the research problem and achieving the study’s objectives.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

Chapter two of this study encompasses an examination of existing research, including an exploration of current theories, empirical, and theoretical framework, examining the research objectives. It is important to note that numerous scholars have endeavoured to distinguish between topics such as cyberspace, cyber threats, cyber-security, cyber warfare, and economic security. The advent of cyber technology has significantly altered the global business environment. For instance, Africa has experienced a notable surge in internet usage over the past decade. However, as the continent advances in digitalizing its business operations, the threat of cybercrime becomes increasingly intricate especially in terms of economic security.

2.1 Theoretical Literature Review

In the dynamic and digital landscape where cyber-crimes thrive, discussions in theoretical research unfold on two distinct levels: one is rooted in theory, while the other is grounded in empirical realities. The first dimension involves generating abstract ideas about natural or social phenomena and the connections between them, essentially formulating theories. Conversely, the second dimension focuses on validating these theoretical concepts and relationships by comparing them to real-world observations. The ultimate goal is to improve the quality of theories by aligning them more closely with empirical evidence. Over time, theories undergo refinement, increasingly converging with observed reality, leading to the advancement of the scientific field (Bhattacherjee, 2012, p. 4).

Scholars in the realm of theoretical research, particularly in the cyber world and its associated crimes, have highlighted challenges in distinguishing between actual observations and the researcher's handling of them (Alasuutari, 2000, p. 39). To address this distinction, it is crucial for the theoretical foundation of policy to have a well-defined research methodology. This methodology should encompass all the steps and actions undertaken by the researcher in conducting observations, along with guidelines governing how these observations are adjusted and interpreted to determine their significance as policy indicators in the digital world.

2.1.1 Deterrence Theory

The research study applied a number of theories in its analytical foundation. Deterrents theory for instance examines how security can be promoted through effective counter cyberc*rime* strategies. Deterrence is a coercive strategy that is based on conditional threats aimed at influencing an adversary to either undertake certain course of action or dissuade them from pursuing undesirable goals (Possony, 1946). This phenomenon explains the state of Africa's crime rate associated with digital activities mainly in the social media as a clear pointer to an existing gap in the continent's digitalization programme.

Cybercrimes have had a detrimental impact on the economic security of the nation, breeding significant insecurity within the economy. According to Kshetri (2019), technology has become ingrained in various business activities, becoming ubiquitous and prompting businesses to adapt by innovating products and services for customers. This adaptation involves developing customer-centric strategies to deliver user-friendly offerings to the target market. However, the pervasive nature of technology also brings a barrage of attacks, compromising the confidentiality, integrity, and availability of business information.

Powell, (2008), postulates that, security scholars have recently given more attention to cyberspace because it has evolved into an important domain of interstate conflict. In 2007 Estonia experienced a campaign of cyber-attacks that temporarily damaged its economy. The state of Georgia experienced a similar cybercrime attacks campaign in 2008/2009 as an element of its war with Russia. The cyber security concept is the process of safeguarding the safety of cyberspace from known or unknown threats. According to ITU, cyber security refers to a collective use of strategies, measures and plans that are geared towards protecting information system, institution and related assets. It plays a significant role in protecting information technology necessary to enhance national economic and security growth. Cyber security refers to measures taken to protect internet, computer networks, electronic systems and other devices from the cyber-attacks. Deterring cyber-attacks is an important component of protecting critical information infrastructure of national cyber security.

Broadhurst (2017) argues that in 2009 the United States and South Korea endured a series of cyber-attacks that some suspect originated in North Korea (or perhaps elsewhere). Some major powers, such as China, have adapted their military strategies to the characteristics of the cyber environment. Real cases of "cyber war" and overt strategizing by government and military analysts around the world have attracted more scholars to the subject of conflict in cyberspace.

Deterrence involves both elements of control and power with ultimate impact on the international sphere (Schelling, 1980). The debate on deterrence gained prominence at the end of World War II, when military power went from being a means to defeat the adversary, to being considered as a key piece of bargaining power employed to avoid wars by means of coercion and intimidation (Schelling, 1980). It was this shift in the understanding of military power that made deterrence possible and a particularly valuable tool in avoiding nuclear conflicts.

According to Angela & Martin, (2012) Securitization theorists assert that successfully securitized subjects receive disproportionate amounts of attention and resources compared to unsuccessfully securitized subjects causing more human damage. A common example used by theorists is how terrorism is a top priority in security discussions, even though people are much more likely to be killed by automobiles or preventable diseases than from terrorism.

Kshetri (2019) suggests that the intricate nature of cybercrimes means that governments, private individuals, and companies may inadvertently become entangled in national or international criminal operations. The perpetrators in this realm include hackers, hacktivists, nation-states, spies, and terrorists.

According to Fitzgerald (2017), individuals who fall victim to cybercrime often experience feelings of violation and vulnerability, leading to heightened fear and anxiety. Clough (2015) observes that the repercussions of cybercrime can have a lasting impact on an individual's mental well-being, particularly if they feel isolated and unable to seek assistance. Mwiburi (2018) discovered that due to the escalation of cybercrimes, many Africans are hesitant to engage with e-commerce platforms. Although they may browse online for products and services, they still prefer to make purchases through traditional means. Consequently, it has been argued that enhancing cyber security is one of the most effective approaches to stimulate commercial activities across Africa.

2.1.2 Routine Activity Theory

According to routine activity theory, cyber threats thrive when there is availability of suitable opportunities and the lack of adequate protection measures. Translating this theory to cyber

technology, shows that the ICT evolution is not without challenges. The advancing nature and falling costs of ICT has given rise to digitalization of economies in Africa. The internet has fundamentally transformed the continents political, economic and social lives. The cybercrime has affected many tools and services such as; the Automatic Teller Machines (ATM) frauds and hacking have been reported in Kenya, Uganda and other sectors of the economy. More importantly, Africa business and customers are deeply engaged in internet online activities, which provide criminals with humble opportunities to strike.

Gagliardone (2014) posits that the growing technological exposure offers its own vulnerabilities and risks. Africa's flourishing economies have an undisputable link to the achievement of technology on the continent. Nevertheless, with these progresses gives way to the threat of hacking, cybercrimes and malware. Generally cyber related attacks usually target weaknesses in the technology infrastructure and processes leading to huge loss of finances and valuable information. According to Ksherti (2019) harmful attacks on systems have been on the rise since malware has gotten more sophisticated and are able to take down any defenses that information technology systems seem to muster. This has led to the growth of other forms of digital crimes such as piracy where illegal copying and acquisitions of games, movies, music and other digital media is acquired.

Scholars have pointed out that asserts that the internet has transformed local and global communication, imbuing it with a transnational and omnipresent character (Fitzgerald, 2017, Bremner, 2017). This blend of attributes has made the internet appealing to individuals inclined towards illicit behavior, posing challenges for governments, businesses, and law enforcement

agencies in regulating online activities. There is concern that if this trend persists, users perceive internet as unsafe and unsuitable for daily use.

Yuchong & Qinghui, (2021) argue that, “cyber risk is not conventional, neither are the threat actors.” Brenner, (2017) affirms that both the increase in the incidence of criminal activities and the likely rise of new diversities of illicit actions pose challenges for legal systems, as well as for security agents. Sukumar & Amoozad, (2023) points-out that, “the cyber infrastructure of the world is transnational; thus, it is illusory to expect it to be effectively managed by a single state, or even by a group of states’ irrespective of whether they have dominant conventional military power and vast economic resources.” Only a transnational framework, based on the consent of all participating states, could be effective in reducing the economic security threat propagated in form of cyber activities.

According to Zdzikot, (2021), cyberspace is more than just internet, information and communications technology and presents peculiar characteristics and challenges. It is supported by critical information infrastructure. The dimensions of cyberspace are wide since it has coverage that traverses from individual, communal, national and to international time and spaces.

According to the 2015 Cyber Security Report by Serianu Cyber Threat Intelligence Team, “the public sector in Kenya lost over KSh5 billion from cybercrime attacks, followed by the financial services sector at four billion Kenya shillings (Okongo, (2021).” The scale and complexity of cyber-attacks is wide ranging. 'Off the shelf' tools mean that less technically proficient criminals are now able to commit cybercrime, and do so as awareness of the potential profits becomes more widespread.

According to Chatterjee, (2019) in the wake of increased terrorist attacks in Africa over the last decades; security, terrorism, business and academic discourse have prominently featured cyber-crime as the primary source of security threats to the economy, critical installations, and societies across the continent. For instance, "Sub Saharan Africa (SSA) as a society is becoming increasingly dependent on the internet, in anything from political processes to the economy, and this makes cyber-attacks attractive means for malicious actors."

The Government of Kenya, (2014) points out that it important to get conversant with the forms and nature of cyber-crime especially since Kenya's national economic security like that of any state is based on several elements, including the health system, government, socio-economic structures and critical infrastructure, which are geared towards achieving the well-being of the state. Kshetri, (2019) suggests that Kenya faces a considerable impact from cybercrime due to its reliance on internet-based services without corresponding advancements in legal oversight.

According to Mwiburi, (2018) cybercrimes in Kenya surged to nearly 340 million by 2021, with increase in malware incidents comprising the majority at approximately 181 million reports. Overall, cybercrime in Kenya increased fivefold over three years. Clough, (2015) adds that another form of cybercrime involves exploiting online platforms to radicalize susceptible Kenyans into violent extremist beliefs, potentially leading to lethal terrorist activities. Marjie, (2013) observes that cybercrime has negatively affected Kenya's economic security, as the country has long lacked adequate mechanisms to combat it.

Ouma, (2021) asserts that the Kenya government has recognized the need to establish a Cyber Coordination Centre where all cases of attack on critical Information Communication Technology (ICT) infrastructure can be reported. In addition, according to Ouma, (2021) the Computer misuse

and Cybercrimes Acts 2018 has sought to align the law to developing forensic procedures when investigating increasing cases of cybercrimes. In reviewing the scholarly arguments this study found gaps to the effect that cyber insecurity is a global responsibility and needs the attention through the whole government approach.

According to Mwiburi, (2018) the emergence of these cyber threats gives rise to the need for up to date strategies and measures to address and manage them. According to Kshetri, (2019) a countermeasure against cybercrime encompasses any action, process, technology, device, or system aimed at preventing or reducing the impact of a cyber-attack on a computer or associated device. Therefore such countermeasures may take either technical or regulatory forms. Technical countermeasures involve recommendations for computer and network users to employ internet security measures, such as using robust and distinct passwords, to safeguard against hackers or intrusions. Regulatory measures, on the other hand, involve legal frameworks that establish and elaborate the criteria for prosecuting cybercrime. Additionally the enactment of the Computer Misuse and Cybercrimes Act 2018 is a major milestone in laying the foundation for legal regulations in matters concerning cyber-activities (GoK, 2018).

The Kenya Government considers national cyberspace security among the top national security priorities in ensuring that her citizen is secure and in facilitating of the growth of her economy as a national interest. Kenyans are increasingly becoming vulnerable to cyber threats because of lack of up-to-date safeguards, against cybercrimes which is considered a serious threat to economic security in Kenya. That said, the complicated and sophisticated nature of the crime as one that takes place in the border-less realm of cyberspace is compounded by the increasing involvement of organized crime groups. It is worth noting that the Budapest Convention on cybercrime and

African Union convention on cyber security and personal data protection laws had influence on the cybercrime law. Kenya, like other nations competes in possession of a robust Information Communication Technology (ICT) infrastructure and therefore the reach and impact of cybercrime is accelerating and becoming more complex (GoK, 2018).

The Kenya Cyber Security Policy is presently coordinated by Communication Authority of Kenya (Okongo, 2021). Key tenets of the policy are computer access training and awareness, cyber safeguards and policies technology economic drivers, ICT Governance and legal framework (Communications Authority of Kenya, 2015). Through these strategies several teams have been established to oversee implementation of cyber technology and security measures as anchored in the law. Consequently, this study will bring awareness that will boost efforts to fight cybercrimes, owing to the fact that recognizing the importance of ICT, the Office of the Director of Public Prosecution (ODPP) has a branch devoted to cyber security crimes under the law. Despite these efforts, the country has faced one of the major international cybercrime cases which have exposed existing cyber weaknesses and gaps in the infrastructure.

The cyber threats have been known to have serious consequences to most societies, especially when they are used to coordinate attacks directed at key national infrastructures. This type of crime mainly used by terrorists and other dissidents are common on web-based systems via internet technology which is easily available online. Owing to these threats some organizations have ceased processing business online for fear of attack and instead have opted for secure modes such as the intranet which utilize Local Area Networks (LAN).

2.2 Empirical Literature Review

2.2.1 Elements of cybercrime as a threat to economic security in Kenya

Generally speaking, scholars have pointed out that as a concept, cybercrime parallels our understanding of traditional crime, both involving actions that result in breaches of national security. The definition of cybercrime has evolved over time and can vary depending on the viewpoint of those observing or safeguarding against it. Gagliardone's (2014) examination of the worldwide cyber threat environment offers a fundamental insight into the complex network dynamics within cyberspace.

Fitzgerald (2017) also suggests that cyber criminals specialize in creating duplicate websites to gather user information which in general terms is called phishing. Phishing involves the use of fraudulent web pages, emails, or text messages to lure unsuspecting users into revealing sensitive information such as passwords and financial details. Mwiburi (2018) confirms that cyber criminals have previously obtained personal information from online users by cloning web pages and using them as bait.

Marjie (2013) also suggests another type of cybercrime termed as a Denial-of-Service (DoS) attack. This constitutes a cyber-assault where a malicious individual aims to disable a computer or another device, making it inaccessible to its intended users by disrupting its normal functions. The objective of a DoS attack is to render a machine or network unusable for its designated users. This is achieved by overwhelming the target with excessive traffic or sending it data that triggers a system crash. There are four main techniques to execute this: Browser Redirection, wherein users trying to access a webpage are directed to a different page with an alternative URL, preventing

access to the original content; Closing Connections, which terminates communication between the sender (server) and the receiver (client).

The hacker closes the established connection, preventing users from accessing resources; Data Destruction: This involves the deliberate destruction of resources by the hacker, rendering them unavailable. This may include deletion, erasure, wiping, overwriting, or dropping tables to destroy data; Resource Exhaustion: The hacker repeatedly requests access to a resource, leading to the overload of the web application. Consequently, the application slows down and eventually crashes, denying users access to the webpage. O'Hanley (2013) suggests that such attacks have increased the cost of conducting business across various sectors of the economy.

Fitzgerald (2017) also highlights another form of cybercrime and that is a malware attack. This is a widespread form of cyber assault wherein malware, typically malicious software, carries out unauthorized actions on the victim's system. Conversely, O'Hanley defines various types of malware, including worms, which are programs designed to continuously replicate or duplicate themselves. Other forms of malware encompass computer viruses, Trojan horses, ransom-ware, malware and spyware. These malicious programs engage in activities such as stealing, encrypting, or deleting sensitive data; manipulating or seizing control of essential computing functions; and monitoring users' computer activities. Clough (2015) described a virus as a program that spreads by infecting files or system areas of a computer or network router's hard drive before replicating itself. While some viruses may be benign, others can damage or destroy data files, while Kshetri (2019) makes the distinction that a Trojan is a virus capable of altering data on a computer, causing it to malfunction or rendering specific data inaccessible.

The robustness lies in elucidating the distinctions between actions for political/ideological purposes and intelligence-gathering, offering a broad perspective. However, an area for improvement is apparent in the lack of direct emphasis on the economic security implications in Africa. This gap aligns with the study's focus on "Cybercrime as a Threat to Economic Security in Africa: The Case of Kenya," revealing the need for a more targeted examination.

Cyber-criminals have taken advantage of the open space as a ply ground to commit crime. Statistics from various sources paint Africa as an environment prone to cyber-related threats due to the high number of domains coupled with weak network and information security. Sayigh (2023) exploration of regional cyber threats, specifically the dissemination of extremist ideas, contributes valuable insights. The solidity lies in addressing regional challenges within cyberspace. However, an area for refinement is apparent in the lack of a dedicated analysis of security implications in Kenya. This gap aligns with the study's focus, emphasizing the need for a nuanced examination of how cyber threats impact economic security in the African context.

Okongo (2021) postulates that cyber threats have found open space in the use of computers and the internet infrastructures which has been used to target government institutions, industries, business and security agents throughout the world. It has been reported on several occasions that the perpetrators often attempt to break into government networks, banking institutions and security offices to gain access to information. In responding to the threats, many countries have taken actions to enhance their national cyber securities. This is because cybercrime has been identified as a threat to national economic security.

The reliance on internet penetration and technological advancement, in Kenya has been exposed to cyber security threats. Okongo (2021), states that Kenya experienced increased cyber-attacks

targeting both private and public sectors. Consequently, due to the increased dependence on ICT has meant that Kenya faces an emerging threat to is infrastructure security. In response to the rising vulnerabilities, Kenya has established a national cyber strategy that is aimed at protecting the nation, (Ziewitz & Brown 2013). Despite the protection measures, the number of cyber-attacks continues to increase. As this study notes, the existing cyber security measures are generally passive in nature and thus fail to transversely cover the full span of operations.

Ziewitz & Brown (2013) confirms that linkage of cybercrime to the growing dependence on computers provides a regional perspective on the origin of cyber threats. The coherence is in connecting cyber threats to regional challenges, setting the groundwork. However, a point to consider is the absence of specific economic security considerations. This aligns with the study's emphasis on economic implications, revealing a gap that the research aims to fill through a more targeted investigation.

Serianu Cyber Security Report (2017), the report estimates the cost of cybercrime in Kenya, emphasizing the economic impact. The strength is in providing local economic insights, but the weakness is the need for a more nuanced study specifically focusing on economic security, emphasizing the gap this research intends to fill. Ziewitz & Brown (2013) explore the origin of cybercrime, linking it to the growing dependence on computers at the local level. The strength lies in understanding the local context, but the weakness is the lack of a specific economic security focus, emphasizing the gap this study aims to fill by examining the economic implications in Kenya. Chuipka (2016) discusses regional challenges and the introduction of electronic services contributing to vulnerabilities locally.

Examining local vulnerabilities, Okongo (2021) thinks that challenges facing Kenyan organisations are that they do not pay adequate attention to cyber security in their organizations. The effectiveness is in bringing attention to local weaknesses (challenges). However, an opportunity for refinement surfaces in the absence of a specific economic security focus. This aligns with the study's emphasis on economic implications, indicating a gap that the research aims to address through targeted exploration.

2.2.2 The impact of cybercrime on economic stability in Kenya

The empirical literature review provides insights into various aspects of cybercrime and its implications for economic security. In this instance, Broadhurst (2017) has asserted that the main argument centers on the global nature of cyberspace and its potential to facilitate unlawful activities. The strength lies in providing insights into the overall dynamics of cyberspace, but the weakness is the lack of specific emphasis on the economic security implications in the African context, creating a gap that this study aims to fill.

Supportively, Gagliardone (2014) asserts that technology or cyber strength lies in exploring the network ecosystem and distinguishing between actions for political purposes and intelligence-gathering globally. However, the weakness is the broad focus on cyber threats without a specific economic security lens, emphasizing the need for a study focusing on economic implications in Africa.

Kshetri (2019) exposes us to further incidences of cybercrime by defining the concept of cyber terrorism which he defines as the premeditated politically motivated attacks against information and computer systems in order to cause catastrophic results to occur to an individual or a group of

people. Attacks are usually carried out by clandestine agents and they do result in death, bodily injury, explosions, plane crashes, and water contamination among other adverse occurrences.

According to Kshetri (2019), cyber-attacks can lead to identity theft, loss of sensitive personal data, and financial harm for individuals. Furthermore, the psychological toll of being a cyber-attack victim can foster feelings of vulnerability and distrust in digital interactions, adversely impacting e-commerce. United Nations Office on Drugs and Crime (2012) the strength of this argument is recognizing the global growth of Web 2.0 and social networking. Yet, the weakness lays in the lack of a nuanced focus on economic security, highlighting the necessity for a study that specifically addresses the economic impact of cyber threats in Africa, particularly Kenya.

Sayigh (2023) main argument revolves around the regional impact of cyberspace and the dissemination of extremist ideas. The strength lies in highlighting regional dynamics, but the weakness is the absence of a dedicated economic security focus, indicating the need for a study emphasizing the economic implications at the regional level.

Angela & Martin (2012) notes that while the argument explores the interconnectedness of the global village with a regional focus, the weakness is the lack of specificity on economic security, creating a gap that this study aims to address by providing a focused analysis of economic impacts in the African context. The development of internet and the expanded access to computer technology has created new opportunities for work and business activities, as well as those who engage in illegal activities. The growth in technology and online communication has not only provided a dramatic rise in the emergence of criminal activities, but has also resulted in the entry of new spate of insecurity. Consequently, cyber threat is asymmetric in nature including its actors.

The growing incidences of criminal events and the likely intensification of new varieties of illegal activities pose challenges for legal systems, as well as for security agents.

Kshetri (2019) argues that cybercrime is prevalent in Nairobi, yet many incidents go unreported. Internet service providers (ISPs) are endeavoring to implement measures to combat cybercrime, such as analyzing network traffic patterns to detect anomalies, filtering suspected malicious content before it reaches users, and offering tools to help customers enhance their cyber hygiene. ISPs serve as a crucial line of defense against the numerous online threats.

According to Chuipka, (2016) it should be noted that the disparity between e-commerce and traditional brick-and-mortar businesses is significant. E-commerce operations generally boast lower overhead costs compared to their traditional counterparts. Without the need for physical storefronts or offices, e-businesses can conduct transactions electronically, thus saving on expenses such as rent, utilities, and staffing. Conversely, traditional businesses often necessitate substantial initial investments in physical space, inventory, and equipment.

Fitzgerald (2017) contends that cybercrime has the potential to harm an individual's reputation. Governments are taking steps to safeguard their citizens' reputations by enacting new statutes, regulations, and establishing dedicated agencies to address this threat. Kshetri (2019) argues that cybercrimes are now universally subject to heavy sanctions by governments in an effort to make e-commerce platforms more popular. Mwiburi (2018) suggests that cybercrimes encompass a range of activities, including unauthorized access, interference, interception, disclosure of passwords, cyber espionage, dissemination of false information, child pornography, cyber terrorism, distribution of obscene images, computer forgery, fraud, and harassment. In Africa, countries like South Africa and Kenya have witnessed notable benefits from e-commerce. South

Africa hosts takealot.com, the country's largest e-commerce platform, while Kenya is home to Kilimall. Despite these successes, Clough (2015) highlights that inadequate regulation has hampered the rapid adoption of e-commerce across the continent.

Chuipka (2016) opines those regional financial losses due to electronic services. However, the weakness is the absence of a dedicated economic security lens, emphasizing the need for a study specifically examining economic implications in the African region. Okongo (2021), Okongo's argument emphasizes the diversity of cyber threats and the lack of attention to cybersecurity in Kenyan organizations. The strength lies in providing local context, but the weakness is the need for a dedicated economic security analysis, indicating the gap this study aims to fill by focusing on economic implications in Kenya.

Okongo (2021), points out that cyber threats have found open space in the use of computers and the internet infrastructures which has been used to target government institutions, industries, and business and security agents throughout the world. It has been reported on several occasions that the perpetrators often attempt to break into government networks, banking institutions and security offices to gain access to information. In responding to the threats, many countries have taken actions to enhance their national cyber securities. This is because cybercrime has been identified as a threat to national security. Ouma (2021) investigates types of cyber threats impacting information confidentiality and integrity at the local level. While providing insights into local threats, the weakness is the lack of a specific economic security lens, highlighting the gap this study addresses by focusing on the economic impact of cyber threats in Kenya.

2.2.3 The response mechanisms to cybercrime as a threat to economic security in Kenya

Angela & Martin (2012) argue that exploring the interconnectivity of the global community, which exposes information to threats, draws attention to local vulnerabilities. This serves to underscore local weaknesses effectively. However, a noticeable area for improvement arises due to the absence of a specific economic security analysis in the African context. This gap corresponds with the study's focus on economic ramifications, suggesting a need for a more nuanced investigation. Despite Kenya's implementation of intervention measures, the issue persists with serious consequences. These measures seem ineffective in preventing or stopping cyber-attacks. Failure to adequately address the problem may lead to future complexities in its management. Consequently, this study aims to identify the security challenges associated with Kenya's use of cyber technology and propose potential solutions. The intricate relationship between cyber technology and insecurity is of significant importance. The advancements in cyber technology alongside the increase in cybercrime present concerns for national security.

Fitzgerald (2017) posits that an innocuous form of interference on computer systems known as spamming has been on the rise. Spamming is the sending of unwanted messages by an outside system to a user’s system or computer. These are usually advertising messages. For quite some time this form of interference has not been a major concern as it was used by genuine advertisers to send unwanted advertising messages to users but lately many spam messages have been containing harmful viruses that attack and damage or steal important data. Clough (2015) posits that piracy is relatively easy to undertake since it may only require the use of Computer Disk (CD) writing software which is available widely within the market. Lewis and Baker (2013) posit of

other kinds of cyber-criminal activity which is known as cyber bullying. This can be defined as the use of the internet to annoy alarm or threaten an individual or a group of people.

Kigen and muchai (2015) argue that cyber bullying is usually accompanied by cyber stalking where an individual is always monitoring another person's social media account or emails after illegally breaching authorization standards. This is usually done when one party wants to acquire some form of control over another. These sorts of crimes are closely related to content related crimes such as child pornography, genocide promoting material and or xenophobic related material.

Chuipka, (2016), notes that, the introduction of electronic services in Kenya has introduced new vulnerabilities, leading to financial losses. The lack of sufficient information technology security expertise and staff in organizations poses a challenge to the security of the cyberspace infrastructure. The main argument focuses on the vulnerabilities introduced by electronic services. The strength is in identifying regional challenges. However, the weakness is the limited focus on specific economic security dimensions. In the context of this study, there is a gap in understanding how regional response mechanisms address economic security in Kenya. Okongo, (2021) points-out that, the diversity of cyber threats in various contexts, including scams, sophisticated attacks, and the lack of attention to cyber security in Kenyan organizations and even Kenyan households.

Ouma (2021) investigates the types of cyber threats impacting information confidentiality and integrity at the local level. Kenya has made great strides to embrace technology in automating its business processes. Additionally, the country has been recognized internationally for innovating *M-pesa* or electronic and mobile money service platform however, this growth seems to be challenged by the evolving threat of cybercrime. Considering the fact that with the existing

measures and strategies to safeguard the ICT sector, cyber security is fundamentally an asymmetric problem. This withstanding, there is indication that there is likelihood of existing gaps in the security laws, poor information security policies or lack of awareness of information security issues, which this thesis is investigating.

Ouma (2021) argues that Kenya has lately been a victim of international cybercrime with the most recent one in 2017 involving criminals from China, America and Europe. This study notes that cyber-incidents in Kenya have caused significant damage. As much as the potential for catastrophic cyber-attacks against critical infrastructures seems likely, hence cyber-security must be viewed as a national security issue. This gap must be closed through effective response by deploying resources on research and development on cyber security. In regards to Kenya, should enact laws suitable to address cybercrime and cyber security to mitigate on the threats.

According to Chuipka, (2016), the most common types of computer fraud include computer operations where intangible assets represented in data such as money transactions are lucrative targets of fraud related to computer. In modern business environment most, financial transactions are processed through computer systems such as financial transaction by use of credit cards and other electronic devices which have become potential grounds operating for organized criminals, (Siegel, Saukko, & Knupfer, 2000). Clearly, the internet has created an atmosphere that offers new opportunities for destructive activities that are currently the subject of consideration that amount to threats to economic security.

Kshetri (2019) notes the absence of relevant data indicating the factors impeding e-commerce growth and their respective impacts. This lack of data complicates the development of policies to promote e-commerce, as essential consumer information is unavailable. Questions arise regarding

whether emphasis should be on domestic or international e-commerce, potentially generating foreign exchange. Moreover, Kenyan consumers face challenges in engaging in online commerce due to the absence of explicit protections for online buying and selling rights.

Siegel, Saukko, & Knupfer, (2000) notes that unlike some countries, Kenya lacks strong laws safeguarding consumers in online transactions, as online trade platforms are not regulated under the Kenya Information and Communications Act (KICA). Consequently, consumers are not covered by Consumer Protection Regulations, leading to vulnerabilities exploited by cybercriminals, as evidenced by the significant increase in cybercrimes from 3.8 million to 10.2 million reported cases.

Lewis & Baker (2013) are of the opinion that the cyber offenses mentioned above must be mitigated through technological innovations that will enable systems to capture evidence of wrong doing against itself and that this evidence must be admissible in court. Nevertheless, internet is an enormous network and this poses a challenge in protecting consumers from its services since attacks may originate from anywhere in the digital ether and taking legal action against perpetrators may be a challenge especially for those with limited resources. Even though the internet has managed to usher humanity into the information age, it has aroused new fears of what might be awaiting users and companies since digital crimes seem to be able to be perpetrated on a grand scale and from virtually anywhere in Kenya.

The failure of the continent to invest in Information Technology (IT) security and cyber security suggests some of the sources of the existing gaps. Consequently, the cybercriminals have cashed on this weakness targeting unprotected devises and luring their unsuspecting customers to fake sites. This is true considering the rapid increase in cybercrime in Kenya which are attributed to

lack of a government owned agency to track and monitor online activities of suspects. The Kenya cyber security laws are week and rarely provide effective remedies to suspects.

Segel, Saukko, & Knupfer, (2000) argues that Kenya is one of Africa's leading digital economies. The country has undergone a digital revolution since the early aught; steady investment in connectivity infrastructure, coupled with an enterprising populace, has seen the country's information, communications, and technology sector grow by an average 10.8 percent in recent time. Much of Kenya's digital success is underpinned by the role of mobile technologies, as reflected prominently in policy documents.

The national ICT policy prioritizes a cyber-technology strategy because most citizens access the internet via mobile phones. The Kenyan government has dubbed its ICT agenda the Digital Superhighway. Through additional investments in fiber connectivity, satellite, and other emerging connectivity solutions, the government aims to expand high-speed internet access nationwide to transform the country, create jobs, and enable growth. The existing literature shows that as technology advance, so is does the threat landscape. Due to this development, the criminals use the same to scale their operations and exploitation of the expanding network.

2.3 Theoretical Framework

This paper utilizes Ole Weaver's conceptualization of Securitization, as outlined in the field of International Relations. Securitization involves state actors redefining certain issues as matters of security. Buzan (1998) describes security as a step that transcends conventional political norms, framing the issue in question as a distinct form of politics.

2.3.1 Theory of Securitization

The world today lacks clear policies on cyber security and the available laws cannot lead to any meaningful action Securitization can thus be seen as a more extreme kind of politics (Buzan, 1998). Therefore, the securitization of a particular issue involves a process that goes beyond the normal political means to resolve the threat that the issue presents. Within the Securitization Theory, the term 'threat' is critical as it determines the existential nature that is behind the move to securitize an issue in order to make it exceptional. Buzan, (1998) refers to the act of raising an issue above normal politics in order to seek a remedy to the existential threat posed to a referent object as a securitizing move.

According to Buzan, (1998) securitization theorists argue that a subject that has been successfully securitized will receive disproportionate attention and resources in comparison with subjects that have not been securitized, even when these other subjects actually because more harm. Paula, (2014) affirms that the key attribute to preventing cyber terrorism is awareness because all a cyber-terrorist looks for is access into a network and one could just be providing them with it through poor cyber hygiene.

The current academic analysts fear the increasing frequency of cyber-crime in Kenya could be a precursor to a larger assault that could deeply impact local businesses and the broader economy (Ouma, 2021). Cyber threats combined destruction of physical and or virtual property with financial crime, propaganda, economic warfare and possibly physical harm to innocent lives.

Paula, (2014), notes that, until recently, in cyber threats in Kenya have been associated with physical acts of violence and crime; for example, killings, bombings, kidnapping, and destruction of property. Starting in the twentieth century the increasing advent of technology, and more

specifically systems controlled by computers, has seen a new form of terror activity for law enforcement to worry about. The key attribute to preventing cyber terrorism is awareness because all a cybercrime looks for is access into a network and you could just be providing them with it through poor cyber hygiene. Therefore, this study tries to address the need for increased awareness of cyber threats on economic security and how can be addressed through security measures such as security awareness, policies, practices and procedures in Kenya.

Evans, (2021) opines that cyber security is now a growing concern to the continent. Gagliardone, (2014) states that as technology evolves, so is the nature and prevalence of cyber threats. With businesses trying to find better ways to link with their customers, cyber security is presents a huge risk with potential to compromise client loyalty and trust. These risks are seen in the way in which cybercrime is defying every prescription.

The growth in ICT, presents exclusive opportunities for monetary service sector expansion in Africa. These advances cover all sides of the financial service sector ecosystem, from data storage and sharing, security, and analytical processing. All these are critical enablers for a booming financial service sector in the continent. For example, despite the political and ethnic conflicts experienced in Kenya, the country has utilized ICT in the economy especially in information and marketing as compared to her East African Community (EAC) states and the wider Africa region. Kenya serves as a communications center for the region, with most of its businesses gradually aiming to establish a regional footprint in ICT development. Kenya's ICT sector has earned from these conditions and a relatively advanced telecommunications sector, supported by three undersea fibre optic cables.

The vulnerabilities of Africa's cyber space to attacks is due to the growing digitalization without a corresponding defence capabilities. The degree of cyber risks is directly linked to the degree of growth in global digitalization. As observed, the institutions dealing with cyber security are not keeping in pace with the rate in which digital technologies are developing. Similarly, enforcement and regulations have equally not moved in tandem to the cyber landscape. Hence a lack of legal framework, infrastructure for enforcement mechanism, monitoring and coordination has not contributed to creating a secure cyberspace.

The cyber-attacks are diverse and emanate from all elements seeking to publicize their political views, criminal organizations seeking financial gain, terrorist groups seeking to inflict economic or political damage, to state-sponsored intelligence and security organizations. Due to globalization and over dependence on ICT, Kenyans is increasingly becoming vulnerable to cyber-attacks because of lack of up-to-date protections.

A literature review conducted in this study reveals gaps highlighting that cyber insecurity are a global concern requiring state attention. It is essential to recognize that security challenges in developing nations share commonalities, with shortcomings in their setups that continue to evolve, shedding light on the situation in African states. Common threads are emerging pertaining cyber crime in developing nations and their mitigation stances. It is worth noting them in order to cut a more pristine picture of the clear and present dangers facing not only a small country like Kenya but the entire continent of Africa.

According to the British consulting firm Ovum, it was projected that by 2022, approximately one billion people in Africa would have access to the Internet. Analysts studying the prevalence of cybercrimes globally had indicated that Internet penetration rates of 10–15% would serve as a

threshold for significant hacking activities (Kshetri, 2013). Many African countries have already surpassed this threshold. Bulent Teksoz, from Symantec Middle East, remarked, “Cybercrime is increasingly targeting emerging economies, where cyber criminals perceive easier targets.” Consequently, numerous African economies have emerged both as sources and victims of cyber threats.

In discussing the rising trend of cyber victimization in Africa, Hamadoun Toure, former secretary-general of the International Telecommunications Union (ITU), expressed the situation as follows: “Currently, cybercriminals view Africa as a secure environment to conduct illegal activities without fear of repercussions.”

In 2016, Symantec detected 24 million instances of malware targeting Africa. A report by Symantec in 2013 highlighted that cybercrime was proliferating in Africa at a swifter pace compared to any other global region. Certain economies within the continent are increasingly appealing to cybercriminals due to the extensive digitization of economic processes. For example, 86% of South Africans frequently utilize online banking services, a figure surpassing that of numerous countries in the Middle East and Turkey.

The rising incidence of cyberattacks in the continent is linked to vulnerable systems and insufficient cybersecurity measures. As per the Business Software Alliance, Africa had two countries with the highest software piracy rates globally in 2017: Libya and Zimbabwe, where unlicensed software accounted for 90% and 89% respectively. Pirated software lacks access to updates from manufacturers, thereby exacerbating the proliferation of malware.

In numerous African economies, cybersecurity is often viewed as a luxury rather than a fundamental necessity. Its significance has not been fully recognized or acknowledged across the

continent. Many organizations reportedly allocate less than 1% of their budgets to cybersecurity, and some even have zero funding allocated to it (Kshetri, 2013).

Despite being prime targets for cyber threats, financial institutions often lack adequate cybersecurity measures. A study conducted in 2009 revealed that 60% of Kenyan banks had vulnerable systems. Furthermore, a 2011 Deloitte study indicated that only 40% of banks in Kenya, Uganda, and Tanzania were adequately equipped to counter cyber threats (Karambu, 2011). Another survey conducted among banks in Kenya, Rwanda, Uganda, Tanzania, and Zambia highlighted the high susceptibility of banks to threats such as hacking, as well as risks posed by employees with inadequate security awareness and malicious insiders.

Another issue stems from the insufficient skills among Internet users to safeguard themselves against the escalating cyber threats. Similar to other developing nations, a significant portion of African Internet users lack experience and technical proficiency. Many are acquiring computers and accessing the Internet for the first time, with a considerable number also facing language barriers, particularly regarding English proficiency. This latter point is significant as most security-related information, instructions, and content are predominantly available in English, rendering cybersecurity products inaccessible to many African Internet users.

The continent grapples with a significant shortage of cybersecurity professionals. Projections suggest that Africa could face a deficit of 100,000 cybersecurity personnel by 2020 (Kshetri, 2015). Similar to the BRICS countries (Brazil, Russia, India, China, and South Africa), African economies encounter economic and institutional obstacles in nurturing cybersecurity expertise. For instance, Cameroon, one of the countries most affected by cybercrime in Africa, has struggled to address the issue due to economic constraints. Reports from 2016 indicated that policymakers

in the country were contemplating initiatives to develop cybersecurity skills. However, there were concerns among policymakers that trainees might potentially misuse the acquired skills for criminal activities after completing the training programs.

Another contributing factor pertains to inadequate legislation and law enforcement. Many African economies operate under lenient regulatory frameworks, providing fertile ground for cybercriminal activities. According to a joint report by the African Union Commission (AUC) and cybersecurity firm Symantec in November 2016, out of the 54 countries in Africa, 30 lacked specific legal provisions to combat cybercrime and handle electronic evidence. In some countries, law enforcement authorities exhibit reluctance to pursue cybercriminals targeting international websites. For example, officials in Nigeria claimed ignorance of cybercrimes originating from the country, dismissing them as Western propaganda. Additionally, there have been reports of elected high-ranking state officials allegedly participating in cybercrimes. In 2003, Nigeria's Economic and Financial Crimes Commission (EFCC) arrested Maurice Ibekwe, a member of Nigeria's House of Representatives, on suspicion of involvement in cybercrime-related activities (Kshetri, 2013).

Cybercriminals also exploit discrepancies in jurisdictional oversight, both within and across borders. After crackdowns on cyber cafés in major Nigerian cities, cybercriminals reportedly relocated to remote regions to continue their activities. With porous national borders and limited state control over territories, cybercriminals can seamlessly shift from one jurisdiction to another, often opting for areas with weaker legal frameworks and enforcement mechanisms. A legal expert from Nigeria's Economic and Financial Crimes Commission (EFCC) observed that as Nigeria

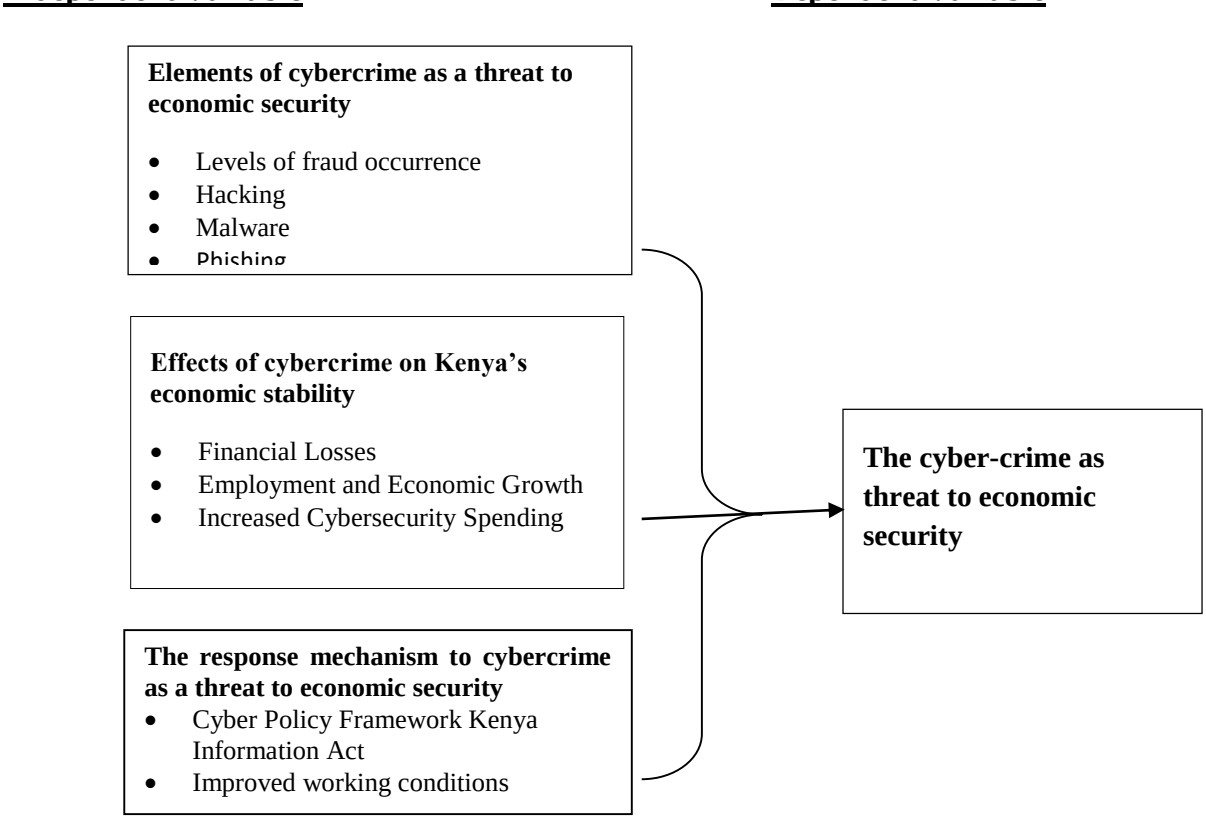
bolstered its anti-cybercrime measures, cybercriminals began migrating to other West African nations.

It must be noted with grave concern that even though developing nations do not have great financial muscle like developed countries, Cyber assaults originating from African nations exert a global impact. Gady (2010) has emphasized the severity of this issue, arguing that Africa's "Cyber [weapon of mass destruction] WMD" poses a direct threat to the world. For instance, in 2010, 80% of PCs used in Africa were contaminated with viruses and malware (Gady, 2010). Cybercriminals frequently exploit these vulnerable computers to orchestrate attacks against targets worldwide.

2.4 Conceptual Framework

The diagrammatic comprise of the independent variable, intervening variable and dependent variable as summarized below.

Figure 2.1: Conceptual Framework



Source: Author, (2024)

The conceptual framework forms the theoretical backbone of this study, offering a systematic approach to explore the impact of cybercrime on economic security in Kenya. By integrating these dimensions, the study aims to provide insights that contribute to the development of informed policies, and interventions necessary to mitigate the economic risks posed by cyber threats in Kenyan context. This framework establishes a foundation for analyzing the intricate interplay of factors influencing cyber threats and their implications for economic security.

This study explores the emerging patterns of cyber technology and economic security threat in Kenya. It provided a background of cyber technology situation in Africa, Kenya ICT environment

and the emerging cyber threats trends manifesting in form of malware software attack that causes harm to computer users and their system. It explores how malware manifests and gains access to computer software without the user's knowledge. The chapter further identifies the various types of malware software and the effects it has on victims. Hence the cyber environment or digital climate is characterized by digital data storage and information network systems. Cyberspace plays an important role in global economy which includes commerce, industry, security, technology and diplomacy.

Kenya utilizes ICT in the conduct of her economic, social and national security activities using the digital technology. ICT continue to have huge impact on all aspects of human development in Kenya. It permits the capture of huge quantities of information and helps speed up the processing and communication of the information. For instance, the government relies on information technology (IT) infrastructure to provide services and improve efficiency of her operations.

2.5 Chapter Summary

Chapter two of this study has encompassed an examination of existing research, including an exploration of current theories, empirical studies, and the theoretical framework, all while examining the research objectives. Numerous scholars endeavored to distinguish between topics such as cyberspace, cyber threats, cybersecurity, cyber warfare, and economic security the chapter has featured a discussion on securitization and deterrence theories in addition to a conceptual framework detailing out the relations between the independent and dependent variables.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter highlights the specific procedures or techniques that were used to identify, process, select and analyze respective data of the topic under study. It discusses the study design, sample site, sample frame and target population. It includes data collection, validity and reliability as well ethical considerations and limitations of the study.

3.1 Research design

This research investigation adopted a mixed methods approach, combining both qualitative and quantitative methodologies to provide a comprehensive understanding of the research problem (Kothari, 2011). In essence, research methodology serves as a blueprint, determining the path toward achieving the intended results. Within this framework, a mixed methods research design was employed, characterized by a strategy that integrates the strengths of both qualitative and quantitative data to explore and analyze complex phenomena. A research design can be defined as the strategy, plan of action, process, or design guiding the selection of specific methods and connecting them to the desired objectives. Methodology encompasses the theoretical rationale researchers use to validate their chosen research methods and designs, ensuring that the mixed methods approach effectively addresses the research questions from multiple perspectives.

This research utilized a systematic review to investigate the impact of cybercrimes on economic security in Africa, with a focus on Kenya. Primary and secondary sources, including academic journal articles and books published between 2010 and 2024, were gathered from databases such

as JSTOR, Science Direct, and Google Scholar. Search terms like "cybercrimes," "economic security," and "securitization of the digital world" were employed to identify relevant studies. Eligible studies underwent review to identify additional pertinent research.

3.2 Study site

The research centered on analyzing how cybercrime affects Kenya's economic security. It aimed to explore not just the cybersecurity threats but also Kenya's response strategies to counter these threats in the digital realm and safeguard the nation's economic stability. The study drew upon secondary sources discussing topics such as cybersecurity, malware, terrorism, and digital threats.

3.3 Target population

The target population was key experts in cyber technology, crimes, economic, defence and national security. Therefore, the target population was a true representative of the target group who deal with the subject matter on a day-to-day. Hence the respondents will include structured questionnaire aimed at key stakeholders in cyber security who included, Kenya Defence Forces, National Police Services, National Counter Terrorism Center, Immigration Department, Kenya Prison Service, Kenya Civil Aviation, Ministry of Foreign Affair, National Intelligence Service, as this proportion of the target population has the characteristics to be measured constitutes as supported by Mugenda (2003).

3.4 Sample size determination

The sample size determination is the process of choosing the number of observations or replicates to include in a statistical sample. In this study, a sample size of 50 was determined based on the need to gather diverse perspectives from key stakeholders involved in national security and

counterterrorism efforts. The goal was to ensure that the sample was representative enough to make valid inferences about the population from which it was drawn (Mugenda, 2003).

The sample was drawn from a pool of key stakeholders, including personnel from the Kenya Defence Forces, National Police Services, National Counter Terrorism Center, Immigration Department, Kenya Prison Service, Kenya Civil Aviation, Ministry of Foreign Affairs, and the National Intelligence Service. A purposive sampling technique was employed to select these 50 participants. This non-probability sampling method was chosen because it allowed the researchers to intentionally select individuals who were most knowledgeable and relevant to the study's objectives, ensuring that the sample comprised experts and key personnel who could provide valuable insights into the research topic.

3.5 Sampling procedure

This method applied ensured that all the different units of the population were very duly represented in the research. This assisted in removing bias on the samples chosen which would have negative affects to the outcome of the study. Such biases would likely negatively affect the quality of data and the resultant study findings of this research (Mugenda,2003).

3.6 Data collection instruments

This research utilized a combination of primary and secondary data, with primary data being specifically gathered through structured interviews. According to Kothari (2011), interviews are frequently the preferred method for collecting qualitative data. Consequently, Key Informant Interviews (KIIs) were employed in this study to effectively capture narrative data and delve deeper into respondents' perspectives.

3.7 Study Validity and Reliability

The study acknowledged the importance of enhancing the validity and reliability of its findings. To achieve this, efforts were made to refine the research instrument by ensuring repeatability and improving internal consistency. As part of this process, the researcher conducted a pretest of the research tool, carrying out a trial data collection and analysis of the questionnaires to evaluate their alignment with the study objectives.

3.8 Data collection procedure

The study drew its data from both primary and secondary sources employing the use of a questionnaire. The necessary steps were taken to ensure that this research is done to the required standards according to the institutional guidelines.

3.9 Data processing and analysis

The information gathered underwent sorting and examination employing document analysis and thematic analysis methodologies, focusing on emerging themes within the research. Document analysis involves qualitative research wherein documents are interpreted to provide insight and understanding into the topic under scrutiny. Thematic analysis, on the other hand, is a qualitative technique aimed at identifying, analyzing, and highlighting patterns or themes within the data. It involves organizing and describing the primary dataset in detail, with each theme capturing significant aspects related to the research question, reflecting patterns or meanings within the data. A coding system facilitated the efficient organization of data for analysis, with specific codes employed to categorize responses.

Following coding, the data underwent analysis using the Statistical Package for Social Sciences (SPSS version 22), enabling quantitative analysis. Descriptive statistics such as means, modes, standard deviations, and percentages were utilized to examine the quantitative data. The findings were presented through frequency tables, bar graphs, pie charts, and narratives, offering a comprehensive depiction of the results (Kothari, 2011).

3.10 Ethical considerations

This research utilized previously published articles and reports, all of which were appropriately cited and referenced. The researcher took care to prevent biases such as data, citation, language, familiarity, country, and multiple publication biases. Furthermore, approval was obtained from the National Defence University of Kenya and authorization from the National Commission for Science, Technology, and Innovation (NACOSTI) was secured for this study. The respondents to the questionnaires were also informed of their right to choose not to take part in the survey. Full confidentiality was maintained especially when dealing with questionnaires and the identity of the respondents were kept private and confidential.

3.11 Chapter Summary

This chapter highlighted the specific procedures and techniques that were used to identify, process, select, and analyze the respective data for the topic under study. It discussed the study design, sample site, sampling frame, and target population. The chapter also covered data collection methods, validity and reliability, as well as ethical considerations and limitations of the study.

CHAPTER FOUR

RESEARCH DATA ANALYSIS AND PRESENTATION

4.0 Introduction

This chapter analyzes the findings, interpretations and presentations of field data aligning with the strategies and measures employed to examine cyber-crime as threat to economic security in Kenya. The collection of data was done through an interview guide, sorted and analysed. Content analysis and document analysis techniques were chosen as a method for data analysis. Scholars have pointed out that document analysis involves a methodical approach to assessing printed or digital materials. Similar to other analytical techniques, qualitative research employing document analysis typically involve scrutinizing and interpreting data to derive significance, enhance comprehension, and cultivate empirical insights (Fischer 2006). Document analysis is integrated with other qualitative research approaches as a form of triangulation, which Denzin (2017) defines as the utilization of multiple methodologies to examine the same subject.

The gathered information was sorted and analyzed using document and content analysis methods to uncover emerging themes in the research. Document analysis interprets documents to understand the topic, while thematic analysis identifies patterns in the data. A coding system was then used to organize the data efficiently. Statistical Package for Social Sciences (SPSS version 22) was used for quantitative analysis, employing descriptive statistics like means, standard deviations, and percentages. Results were presented through frequency tables, bar graphs, pie charts, and narratives for clarity.

The target population for this study included key stakeholders from the Ministry of Foreign Affairs, Kenya Information Communication Technology Authority, Information Communication Technology, Kenya Defense Forces, National Police Services, National Counter Terrorism Center, Immigration Department, Kenya Prison Service, Kenya Civil Aviation, National Intelligence Service and Parliament. In addition to the above, inferential statistics used to establish the predictive control of the study model specified by the following equation:

$$\mathbf{Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon}$$

Whereby:

Y = *Threats to economic security*

X_1 = *Impact of cybercrime on economic security in Kenya*

X_2 = *Contributors of cybercrime as a threat to economic security in Kenya*

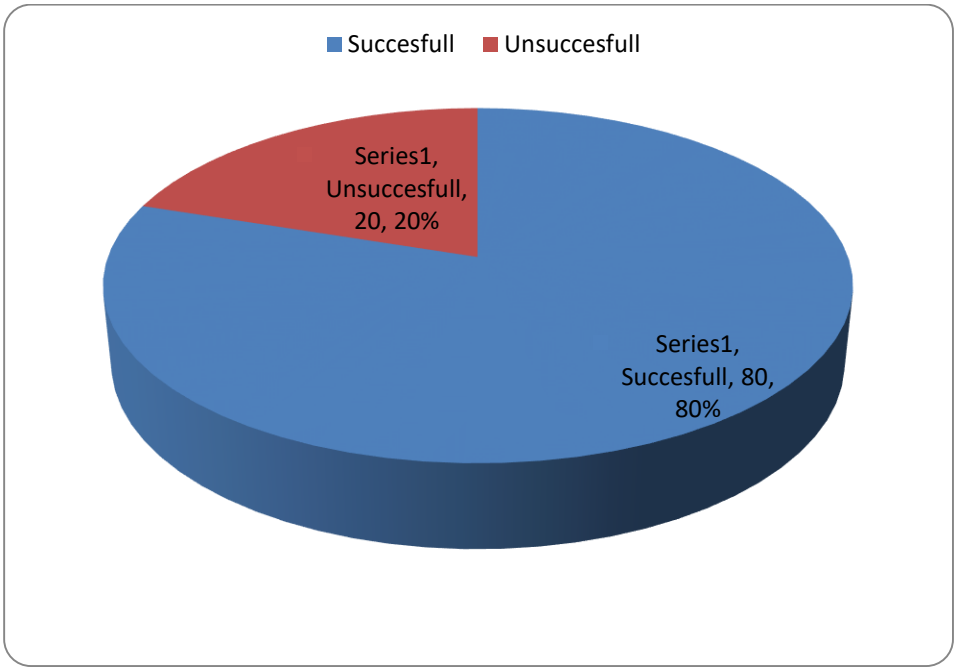
X_3 = *Response mechanism to cybercrime as a threat to economic security in Kenya*

ε = *Erroneous variables*

β_0 = *Mathematical intercept*

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

Figure 0.1: The return rate



Source: Field Data (2024)

Figure 01 above shows the study successfully interviewed 80 percent of the respondents. This response rate was possible as a result of actively pursuing the respondents, proper orientation of the them in to the study, accessibility of many respondents at the time of the study, the ability of the researcher to effectively apply proper research technique in the study and finally because of proper institutional research guidance.

4.1 Personal Profile

This section gave the general profile of the research findings.

4.1.1 Age distribution

The respondents were asked to indicate their age, and hence the ages were put into four classes of nine years difference.

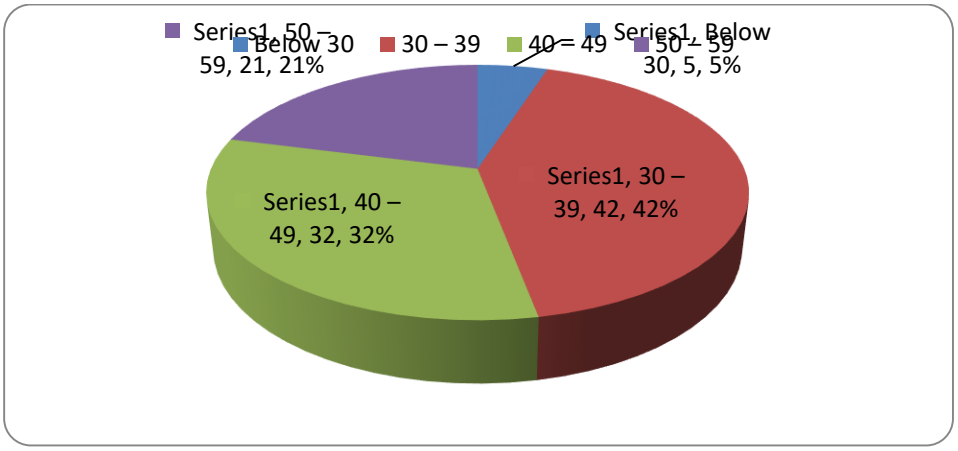
Table 0.1: Age of Respondents

Age (years)	**Frequency**	**Percentage (%)**
Below 30	2	5
30 – 39	16	42
40 – 49	12	32
50 – 59	8	21
Total	**35**	**100**

Source: Field Data (2024)

The results as presented in Table 4.1 shows the distribution is higher among the younger respondents aged 30 – 39 at (42%), followed closely by the middle-aged group of 40-49 years.

Figure 0.2: Age distribution



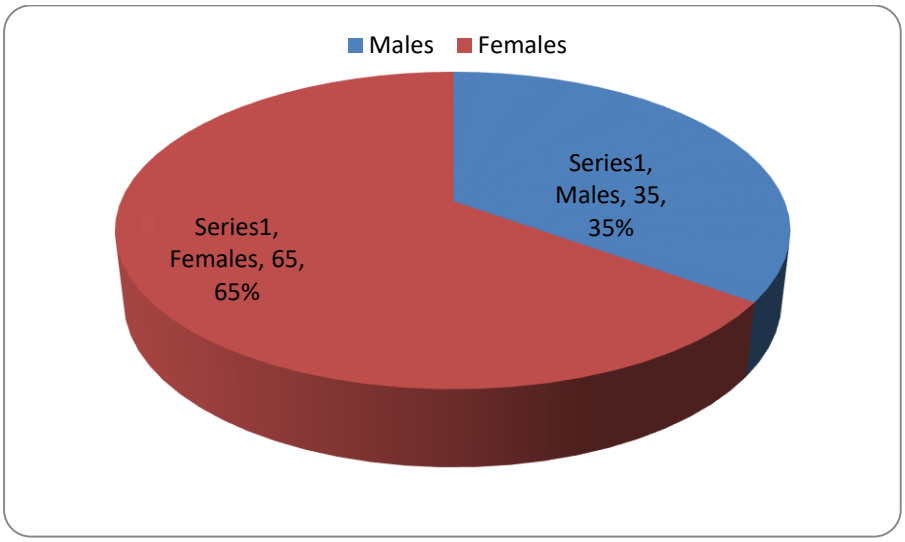
Source: Field Data (2024)

This Figure 4.2 shows the age distribution of the respondents, an indication that the mostly young people are the most exposed to cyber related activities.

4.1.2 Gender distribution

The 50 respondents were to indicate which gender they are and from the 35 who responded and as in the results in Figure 4.3, that is, 25 (65 percent) were male and 13 (35 percent) were female.

Figure 0.3: Gender of respondents



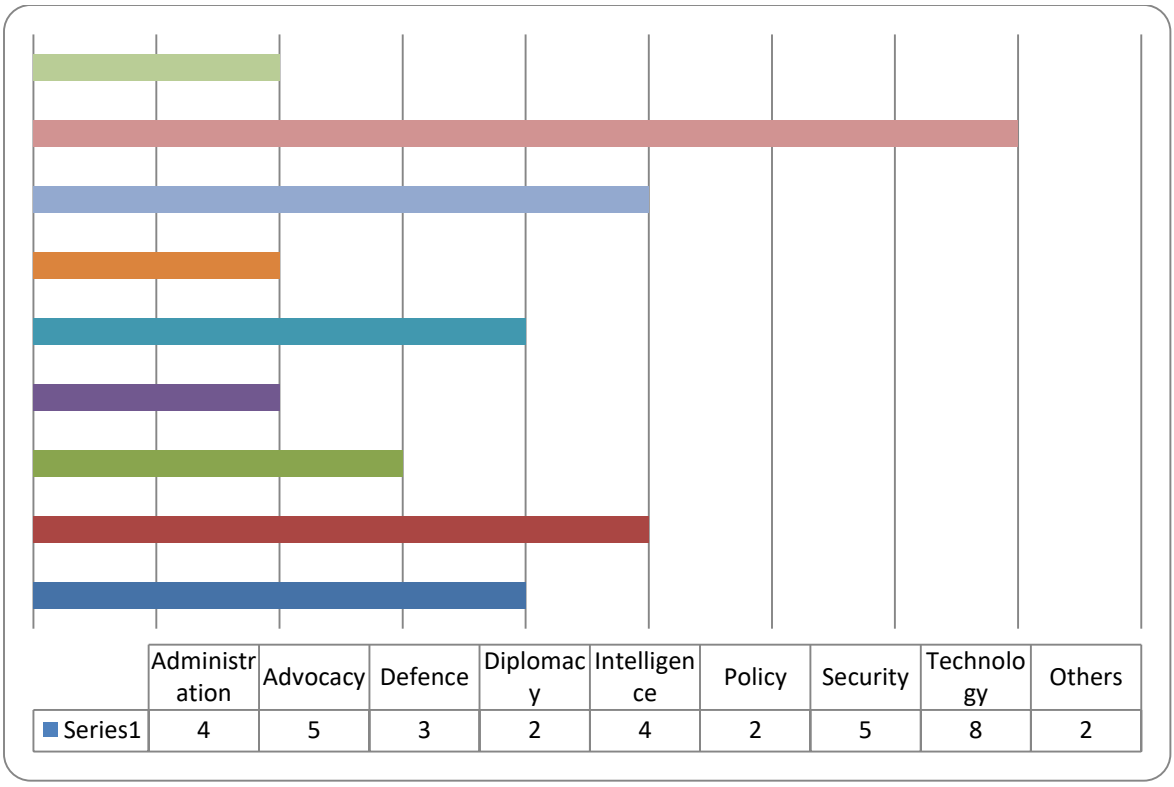
Source: Field Data (2024)

This Figure 4.3 shows the gender distribution of the respondents, the number of males that responded was higher than that for female. Even with the Kenyan gender rule factor is constant, more male professionals are involved with Information Communication Technology sector directly and are therefore more likely to be affected by or involved in cybercrime.

4.1.3 Occupation Distribution

The respondents were requested to indicate their occupation of origin.

Figure 0.4: Distribution by occupation office



Source: Field Data (2024)

Figure 4.4 shows that when it comes to the cyber technology and insecurity in Africa (Kenya), the most directly affected occupation were those from the technology sector (8) and the security sector (5), and advocacy (5) respectively.

4.1.4 Designation

The respondents were asked to indicate their job designation, and hence the designations were put into seven main categories based on their job description.

Table 0.2: Designation of Respondents

Designation	**Frequency**	**Percentage (%)**
Executives	3	9
Manager	10	28
Personnel	8	23
Supervisors	5	14
Technicians	6	17
Others	3	9
Total	35	100

Source: Field Data (2024)

The results as presented in Table 4.2 show the distribution is terms of designation, highest being managers (28%) and indication that they are designation that most interacts with cyber issues.

4.1.5 Duration in office

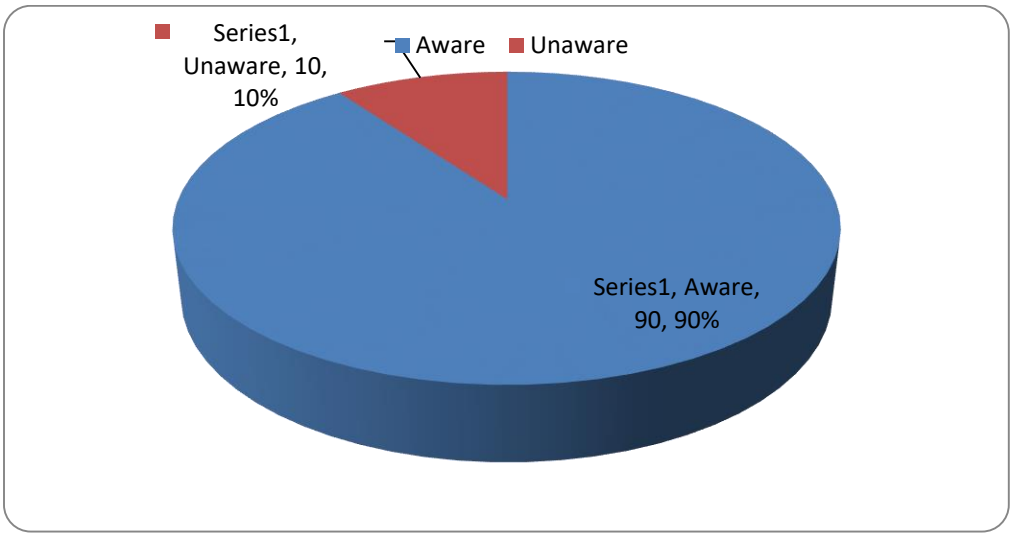
On number of years served in their respective organizations, the majority of the respondents had been in service for at least 25 - 30 years (17 percent), while the lowest numbers had served 1 - 6 years (8 percent). This data assured that the participants had a sufficient experience and understating of the field of study and that data was reliability. Implications of working long especially in same organization.

4.1.6 Concept of Cyber Crime

In seeking to search for the cybercrime, the targeted respondents were to respond on whether they were aware of the cyber threat concept. The results were that that 90 percent were aware of it as

a concept and they had at least experienced it in their line of duty. Only 10 percent were fully unaware of it as they could not define it accurately.

Figure4.5: Awareness of cyber threat concepts



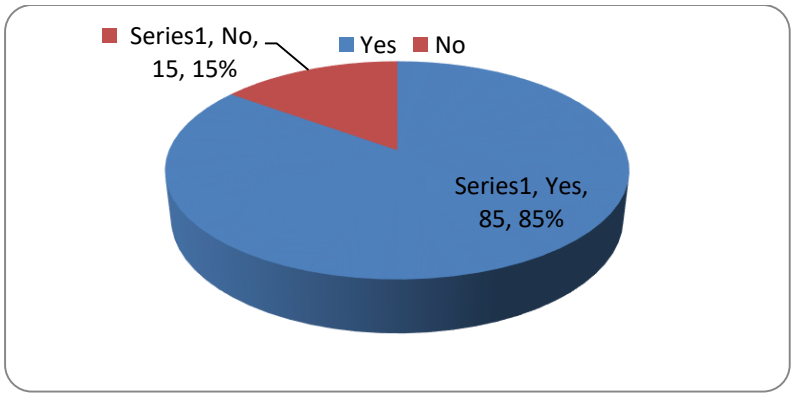
Source: Field Data (2024)

The respondents were asked of their awareness of the concept of cyber-crime; the responses are presented in Figure 4.5.

4.1.7 Witnessed any Form of Cyber Crime

In search for the cyber-crime and national security in Kenya, the targeted respondents were to respond on whether they had experienced (witness) cybercrime.

Figure 4.6: Cyber-attacks witness



Source: Field Data (2024)

The Figure 6 shows that 85 percent had witnessed or experienced cyber-attacks in their line of duty 15 percent stated that they had not yet witness cyber terrorism. Clough (2015) opines on the aforementioned issue by stating that integrating business with the computer world is tempting since it can increase issues of security, efficiency and even anonymity but these are also qualities that can expose the soft underbelly of a system and lead to issues arising such as rapid fraud, money laundering and phishing attacks. According to Lewis and Baker (2013) the internet has facilitated illegal activities in this way: it has maintained existing patterns of harmful activities such as drug trafficking, hate speech, pornography and even bullying.

4.2 The case of cyber threat and economic security in Kenya

This study aimed to determine the cybercrime threat to economic security. The study found that cyber threats are on the increase and are being experienced from all organizations as shown in (Figure 4.6). One of the core priority areas for the government is to utilize e-economy capability to create employment and wealth as part of national development strategy in achieving Vision

2030 ICT flagship on security of the individuals and of property. This goal has been realized through adoption of appropriate technologies such as mobile banking, internet and broadband communications which connects the country to the global village.

4.2.1 Prevalence of cyber technology threats in Kenya

The respondents were asked to identify the prevalent type of cyber-attack they most experienced.

Table 0.3: Prevalence of cyber threat

Type of cyber attack	Frequency	Percentage (%)
Frauds	8	23
Hacking	4	11
Malware	5	14
Phishing	6	17
Pornography	3	9
Spyware	4	11
Steganography	2	6
Others	3	9
Total	35	100

Source: Field Data (2024)

This section shows that that majority of the cyber-attacks consists of cyber fraud (23%), phishing (17%) and the evidence of the research data are interlinked with the findings of the study as shown in Table 4.3. This section aimed to identify the prevalent type of cyber-attack they most experienced in the key respondents respective organization. The findings on Table 3 were in

agreement with the similar PWC (2015) that showed that in today's unstable economic environment, the opportunity and motivations to commit frauds have been on the rise. In addition, the (Table 4.3) aligned with the revelations of Mallory, (2017), who stated that cyber threats and cybercrime are a crime associated with internet technology which concerns citizens, governments and industries where crime manifests in the form of either cyber stalking, phreaking (arching to obtain free telephone calls), piracy, cyber terrorism and cyber pornography. In view of this understanding, it is therefore possible to argue that all stages of computer use are vulnerable to criminal activity either as a key target or agent of cyber fraud.

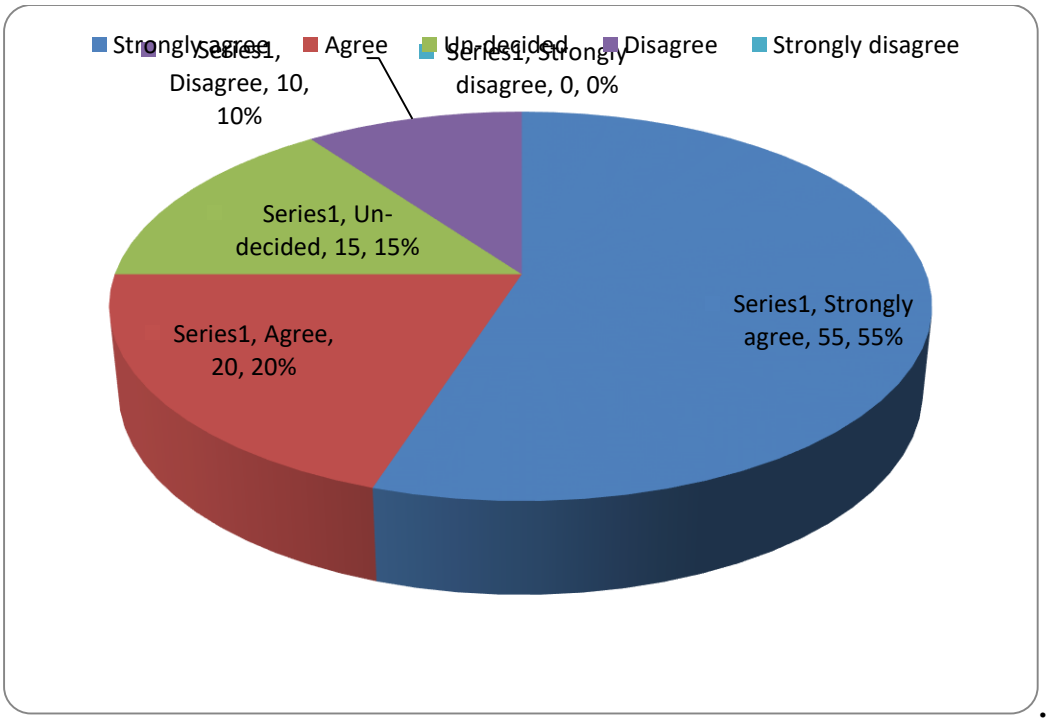
Finally, this study notes that based on the data (Table 4.3) this research infers that cyber attacks are on increase as shown by the number of very many cases identified and experienced in various organizations as illustrated by Figure 4.4. This therefore confirms that a wide array of threats to national security exists as a whole and perpetuated by cybercriminals as pointed out by a respondent who stated that most of those involved with cybercrimes are youths who have found an easy way of live by hacking into organization accounts to gain information or money.

In addition, this chapter notes that the majority of ICT managers are between the ages of 30-49 years who account for 80 per cent as shown in (Table 4.1), yet cybercrime perpetrators are youths, which clearly points to a disconnect between the vulnerable youths and the ICT policy makers. As the country moves towards joining machine controlled automated economies through computer and internet service provisions, this has not been without the challenge of crimes and serious collateral damage coming along with the era of advanced technology. Cyber threats are on the increase and have attracted fraudsters from within and outside the country who have managed to gain easy access to the system with impunity.

4.2.2 Cyber insecurity has a direct influence on economic security

The respondents were asked to identify if cyber insecurity has a direct influence on a country's economic security.

Figure 4.7: Cyber insecurity and economic security



Source: Field Data (2024)

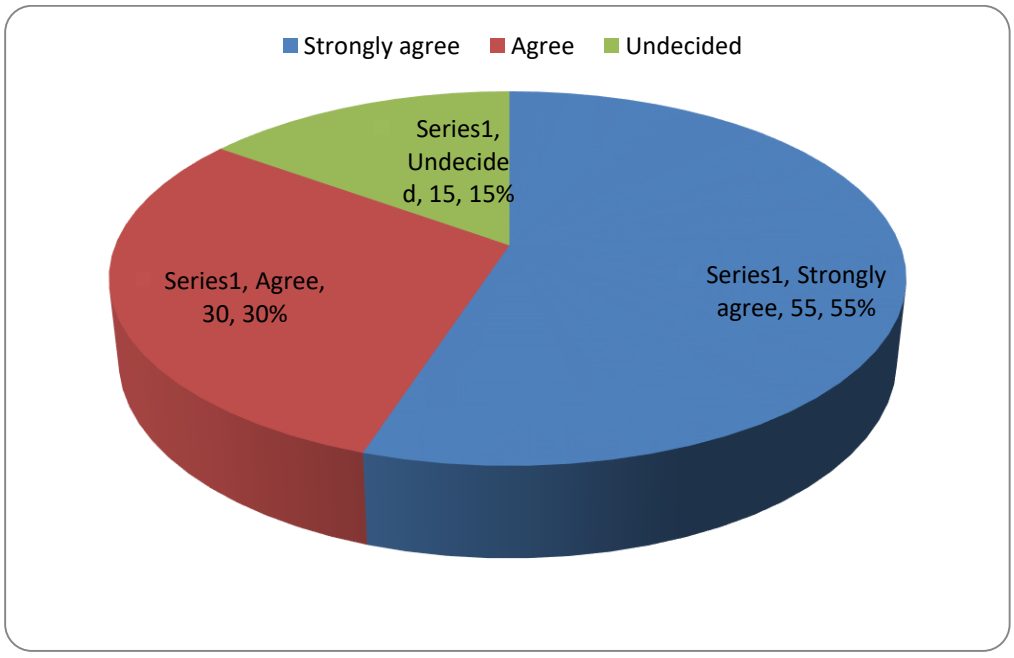
The outcome from a population of 35 the main respondents revealed that, strongly agree (55%), Agree (20%), Undecided (15%) and finally Disagree (10%). This research finding were confirmed by Internet Security Threat Report (2013), that revealed that cyber threats is an increasing global phenomenon, the crime is increasing at a faster rate in Kenya than in any part of the world. Most experts approximate that 80% of individual computers on the African continent are infected with viruses together with other malicious software, (Ranz-Stefan Gacy, 2010). The cyber threats rate in Kenya is associated with digital use especially in the social media and the face book which is

the highly visited website has been identified as the most popular crime zone. The major crimes perpetuated include cyber bulling hate speech in form of short text messages, hacking, phishing and many others are a serious threat to national economic security. This thus aligns with the results findings in (Table 3).

4.2.3 Cyber threats are currently on the increase, now than ever before

The respondents were asked to identify if cyber threats are currently on the increase, now than ever before.

Figure 0.8: Incidences of Cyber threats

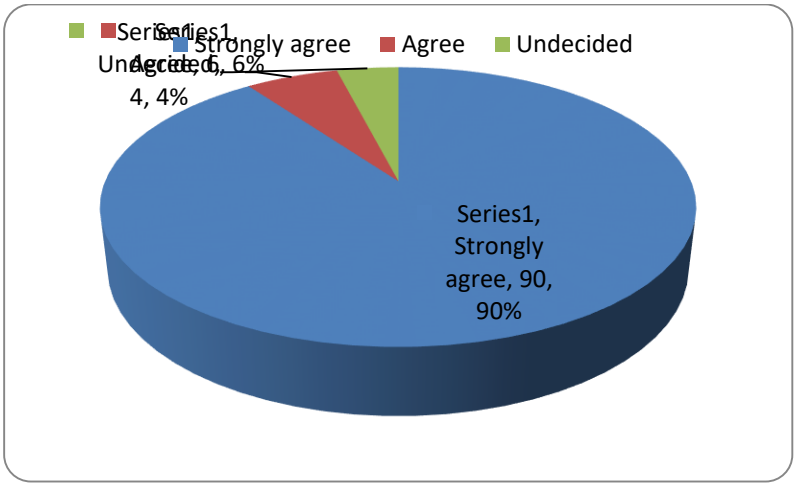


The Figure 4-8 shows the outcome from a population of 35 participants showed that, strongly agree (55%), Agree (30%), and Undecided (15%).

4.2.4 Cyber threats and current economic challenges

The data analysed showed that (90%) of the respondents strongly agreed that the current economic challenges acted as a great motivator for cyber threats.

Figure 4.9: Justifications for cyber threats



Source: Field Data (2024)

The Figure 9 results are in agreement with Siegel, *et*, *al*., who state that most common types of computer fraud include computer operations where intangible assets represented in data such as money transactions are lucrative targets of fraud related to computer. Based on these findings (Figure4- 7, Figure 4-8 and Figure 4-9), this section infers that the reliance on internet penetration and technological advancement, exposes Africa to cyber security threats, for instance Kenya has witnessed increased cyber-attacks targeting both private and public sectors. Clearly as shown in (Table 4.3), as proved by the fact that the Country is highly dependent on the internet to transact major businesses it thus stands the risks of attacks as confirmed from these findings.

The study infers that Kenya currently experiences growing cyber frauds involving mobile banking. Since most users have little knowledge on cyber security, they are most likely to fall victims of

internet frauds. These attacks are mostly common and are relatively easy to execute and has substantial effect on the target. Often, the perpetrators of these attacks use computer programs network tools referred to as Low Orbit Ion Cannon (LOIC) and target a specific website or network. These stress tools work in the form that it overlord's the server with of the target with large data hence temporarily disconnecting the network or webpage. As result of this growth, Kenya has continued to experienced several mobile money thefts perpetuate through malware attacks and personifications of account. As banks embrace e-finance services, hackers are busy fighting to exploit weaknesses in mobile money security controls with an aim to steal.

Kenya has gone ahead to develop strategies to respond to the rising cyber security threats by adapting to internationally recognized standards. Recognizing the importance of ICT in economic development, Kenya has chosen to seek partnerships with actors in the digital world to develop a strategy based on their experiences on the risks. Aseries of cyber incidents that occurred in Kenya in 2023 tested the cyber security and resilience of the rapidly digitalizing country. These events affected government service provision and shook Kenya's digital financial ecosystem. By no means the first, they certainly were the most significant cyber-attacks the country has yet faced. The government has previously dealt with defaced websites and alleged breaches by foreign actors. Financial systems, banks, and *M-PESA* alike have been subject to cyber-related threats and vulnerabilities. Some organizations such as Safaricom and the Communications Authority of Kenya are facing a class action lawsuit over SIM-swap frauds.

4.3 Elements of cybercrime as a threat to economic security in Kenya

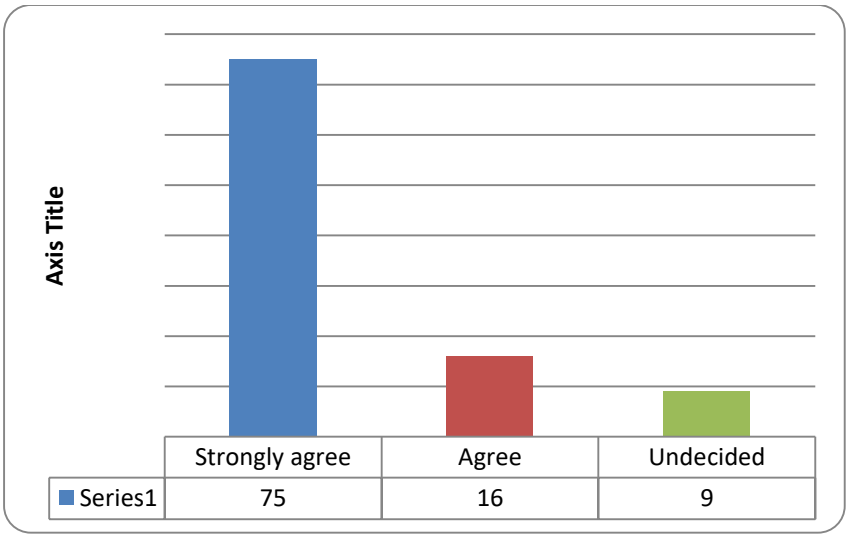
This study summed a wide array of threats to government, business, individuals, and society as a whole perpetuated by hackers, criminals, terrorists, commercial organizations, and nations that

adopt cyber strategies for financial, ideological, political or military gain. The malware attacks are common and target critical mobile and internet banking infrastructure which are presently on the rise. Malwares presents in several forms such as Trojans worm called Dridex and Zeus malware which are very effective. These types of malwares are known to compromise targets making them easy to access sensitive information on the network that lead to economic losses.

4.3.1 Patterns of cyber technology threats

The respondents were asked to identify whether there was an emergent pattern of cyber technology as an economic security threat in Kenya. The outcome from a population of 35 participants showed that, strongly agree (75%), Agree (16%), and Undecided (9%).

Figure 0.10: Increase in pattern of cyber threats



Source: Field Data (2024)

This section infers, based on (Figure 4.10), which the threats of cyber-attacks have greatly increased with development in information technologies which are complex in nature. Cyber

threats have been known to have serious consequences to most societies, especially when they are used to coordinate attacks directed at key national infrastructures.

Evidence shows that Kenya continues to lead in mobile money usage across Kenyan banks ranged from insider threats to spear phishing and ransomware attacks. The banks have continued to be a target through their vulnerable web applications, Internet and Mobile banking platforms which have attracted cybercriminals. While the attack vectors may differ, the execution of the attacks is often the same. It is paramount that local banks invest in mechanisms to Anticipate, Detect, Recover and Contain cybercrime. The financial cooperatives Sacco's and microfinance institutions are rapidly growing in Kenya. However, these organizations have paid much attention to customer satisfaction and reducing costs that they tend to neglect investment in cybercrime prevention.

This section notes that from the start, it's important to note that the growing prevalence of cyber threats, hazards, and attacks in Kenya is increasingly viewed as an imminent and significant national security concern. This is exacerbated by the heightened vulnerability of critical infrastructure due to increased cyber connectivity, allowing cyber terrorists to potentially disrupt systems through attacks. The banking industry ranks just below the government in terms of vulnerability to cybercrime. Due to the substantial amount of data exchanged during financial transactions, the multitude of participants involved, and the complex network infrastructure, it stands out as particularly susceptible to cyber threats. The legal and forensic specialists currently highlight the nation's insufficient technical knowledge, tools, and resources, all of which impact the effectiveness of investigations and legal proceedings. Most respodents emphasizes that in cybercrime litigation, identifying the culprits remains the primary challenge for investigators.

4.4 The response mechanism to cybercrime as a threat to economic security in Kenya

The study sought to find out response mechanism to cybercrime as a threat to economic security in Kenya. The majority of the respondents agreed that there exist measures, policies and strategies on cyber security which provide guidance on cyber security and safety measures. A total of 60 per cent strongly agreed that Cyber Security Policy has helped in mitigating cyber-attacks, 20 per cent agreed while 10 per cent were not aware. About 15 per cent were able to identify Cyber Security Policy and Strategy of 2014 and 70 per cent not able to precisely name any policy while 20 per cent were not sure.

On the basis of these findings (Section 4.4.1) above, Kenya has policies and strategies to contain cyber threats. In addition, most African states have equally adopted different frameworks to contain the threats peculiar to their environment. Most African States such as Kenya, Uganda, Cameroon and Botswana have started to enact cyber legislations and establish sub-regional collaboration instruments to combat cybercrime. Senegal and Morocco are contemplating on joining the AU Convention. On the other hand, West African nations of ECOWAS are considering to adopt the "Commonwealth Model Law on Computer Related Crime and the Council of Europe's the Budapest Convention on Cybercrime and Directive on Fighting Cybercrime."

4.4.1 The Cyber Security Measures in Kenya

The respondents were asked to list the key counter cyber security measures and strategies applied in Kenya.

Table 0.4: Cyber security measures in Kenya

Cyber security measures	**Frequency**	**Percentage (%)**
Central Bank of Kenya Cyber Guidance	7	20
Cyber Policy Framework	2	6
Cyber Regulatory Framework	4	11
Cyber Security Governance	5	14
Kenya Information Act	7	20
Kenya Information and Communications Act	6	17
Kenya National Cyber Strategy	3	9
Others	1	3
Total	**35**	**100**

Source: Field Data (2024)

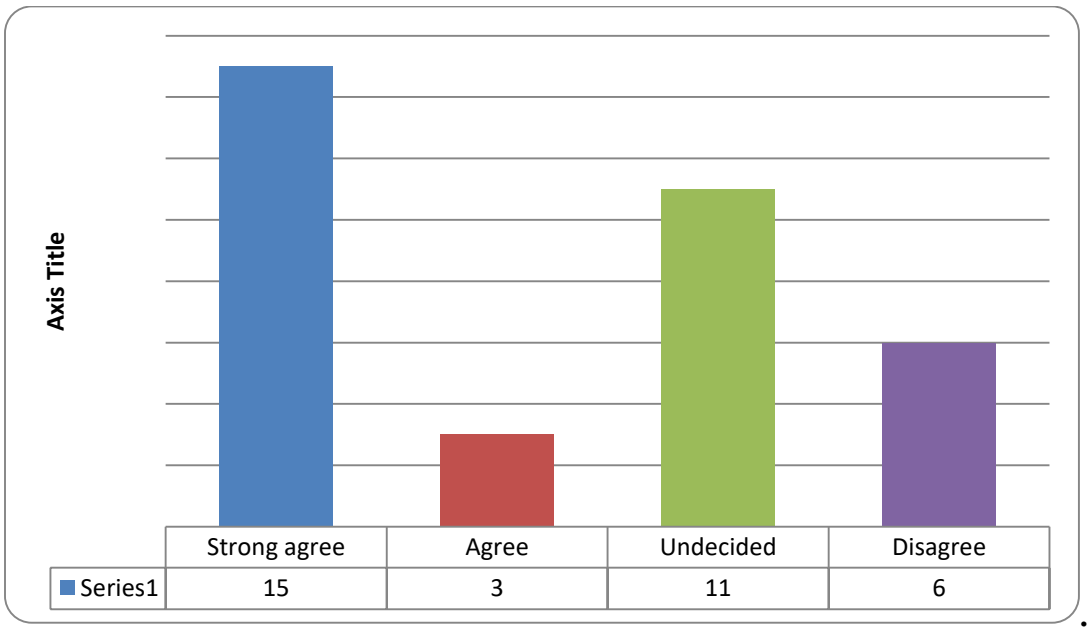
This shows that the findings of the existence of the cyber security measures in Kenya and the evidence of the research data are interlinked with the findings of the study as shown in Table 4.

The findings in (Table 4.4) are similar to those made in Cyber Defence East Africa 2017 Conference, which discussed the different measures taken by Kenya, which included the necessary institutions and legal framework addressing cyber threats facing the country. The strategies include the involvement of international organizations, national institutions and stakeholders. The measures include developing cyber capacity and national institutions to provide a secure and safe cyber environment. Among the achievements is the development of the Kenya National Cyber Security Master Plan 2017/18, response centres and enacted laws to secure the ICT infrastructure against emerging threats.

4.4.2 Achievements in the fight against cyber threats

The respondents were asked to identify whether there were achievements in the fight against cyber threats.

Figure 0.11: Achievements in the fight against cyber threats



Source: Field Data (2024)

The outcome from a population of 35 the interviewed respondents revealed that, strongly agree (15), Agree (3%), Undecided (11) and finally Disagree (6%). This section notes that those who agree (Figure 4.11), majority stated that Kenya gone ahead to develop national cyber security framework and legislation for electronic identification. They have strengthened their law enforcement skills and capacity to successfully fight cyber threats.

This research finding were confirmed by who found that Kenya, through the Communication Authority of Kenya had established a consumer awareness programme as a component of national cyber security initiative and so far the initiative had been successful in thwarting cyber threats.

The East Africa Community (EAC) states have also followed the example and are on discussions to establish a cyber-science centre of excellence. Kenya had planned to establish a cybercrime laboratory referred to as forensic lab to be used by national police, but this was not actualized due to corruption. More support of the findings in (Figure 11), for the majority of the respondents, that (15 strongly agreeing and 3 agreeing), evidence was found in the Kenya Cyber Security Policy is presently coordinated by Communication Authority of Kenya.

On the other hand, the respondents who were undecided (Figure 4.11) stated that the vulnerabilities of Kenya's cyber space to attacks is due to the growing digitalization without a corresponding defence capabilities. The degree of cyber risks is directly linked to the degree of growth in global digitalization. These sentiments were echoed by Serianu Consultants in Cyber Security (2015) who stated that the institutions dealing with cyber security are not keeping in pace with the rate in which digital technologies are developing.

The respondents (Figure 4.11) who were undecided on whether there were achievements in the fight against cyber threats, states that, despite these efforts, the country has faced one of the major international cybercrime cases which has exposed existing cyber weaknesses and gaps in the infrastructure. This outcome (Figure 4.11) seems to correspond to the fact that in December 2014, the country witnessed intrusion into its cyberspace by several foreigners from Thailand and China nationals who were arrested in Nairobi and found in possession of equipment believed were to be used for hacking into ICT networks. The group intended to hack into Safaricom *M-Pesa* (mobile money transfer) system, bank accounts including Banks Automatic Teller Machines (ATM) (Agence France-Presse 2014), (Otuki, 2014). According to the Kenya Police, the suspects were

charged with the offence of operating telecommunication facility which was not licensed (Daily Nation, 2015).

This section aimed to further expound on the approaches to counter cyber security measures and strategies advanced in Kenya, as shown in (Figure 4.5, 4.8, 4.9, 4.10 and 4.11). Whereas the Country continues to lead in mobile money usage across Africa, with this growth, comes a whole new set of cyber threats; mobile malware, third-party apps, unsecured Wi-Fi, risky consumer behavior among others as outlined in Table 3. Therefore, whether or not an institution uses proprietary or third party mobile applications, pose risks to the systems which are still inherent.

In addition (Figure 4.10 and 4.11) was recently supported by the fact that The Kenya Revenue Authority (KRA) sued internet giant Google following a mystery hacking of the taxman's systems. Hackers breached the Kenya Revenue Authority's systems, prompting an investigation. KRA detectives are engaged in a landmark court battle with Google over access to an email at the centre of the hacking. The Directorate of Criminal Investigations has obtained a court order granting it access to an email address used by the hacker. The KRA has served the order to Google's local subsidiary, but the American firm says it is not in a position to assist in the probe.

The (Figure 4.10 and 4.11) is corroborated by the fact that in the month of February 2018, financial institutions suffered major cyber-attack and this confirms that attacks targeting Kenyan banks ranged from insider threats to spear phishing and ransomware attacks. It is therefore evident that the Banks are the most targeted because of their adoption of digital platform in most of their processes, and thus these points to the possibilities of weaknesses in the cyber protection systems. Similarly, the financial cooperatives Sacco's and microfinance institutions are equally affected.

One respondent stated that, in recent years, Kenyan financial establishments have suffered substantial financial losses due to cybercrime. Major attacks have been directed at prominent banks like the National Bank of Kenya, the Kenya Revenue Authority, the Commercial Bank of Africa, the Cooperative Bank of Kenya, and the Equity Bank. The financial Impacts of these attacks vary widely, spanning from hundreds of thousands to millions of dollars. To illustrate, the NBK experienced a loss of KES 29 million ($280,000), the KRA suffered a loss of KES 4 billion ($40 million), the CBA faced a loss of KES 90 million ($900,000), the Cooperative Bank of Kenya incurred a loss of KES 157 million ($1.57 million), and the Equity Bank saw a loss of KES 1.3 billion ($13 million). These significant losses underscore the importance for financial institutions in Kenya to prioritize cyber-security, aiming to mitigate further financial harm and safeguard customer data.

Some respondents quoted the fact that in 2017, one of the most notable cyber-attacks in Kenya targeted the National Bank of Kenya (NBK), resulting in the theft of KES 29 million ($280,000) from the bank's infrastructure. Employing sophisticated methods such as phishing emails, the hackers gained unauthorized access to the bank's system, facilitating the transfer of funds to multiple accounts. This was supported by Okongo (2021), who stated that in 2018, the Kenya Revenue Authority (KRA) disclosed a staggering loss of KES 4 billion ($40 million) due to a cyber-attack. Utilizing the WannaCry malware, the perpetrators breached the authority's system, compromising sensitive data. To mitigate further harm, the KRA was forced to halt its operations, incurring substantial financial repercussions. XXX affirmed that in 2019, the Commercial Bank of Africa (CBA) disclosed a loss of KES 90 million ($900,000) attributed to a cyber-attack. While specific details of the incident were not provided, it was indicated that the attackers employed ATM malware to siphon funds from the bank's automated teller machines.

4.4.3 New Measures to Counter Cyber-crime

In summary to the banking situation, Kenyan banks have incurred significant financial losses due to cybercrime in recent years. However, both banks and regulatory bodies have taken proactive measures to bolster cyber-security within the industry. Directives have been issued, specialized cyber-security units established, and cutting-edge technologies like Artificial Intelligence (AI) and block-chain embraced to mitigate cyber-threats. Through collaborative efforts with various stakeholders, Kenyan banks are striving to prioritize cyber-security and mitigate future financial losses.

4.5 Chapter Summary

This chapter reveals that a prevalent cause of susceptibility to cyber-attacks among both individuals and organizations stems from a lack of awareness regarding necessary security measures among customers and employees. Law enforcement's efforts to address this issue have been hindered by insufficient training, as both police officers and judicial officials struggle to grasp the technical complexities involved.

The evidence presented here underscores the growing apprehension among individuals, companies, organizations, and governments about the risks posed by cyber threats in an era marked by extensive use of cyberspace, the internet, and digital applications. Consequently, cyber threats encompass various forms of malicious activities targeting the cyber domain, including unauthorized access, manipulation, interruption, destruction, and sabotage of the physical infrastructure supporting information processing, communication, and storage.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.0 Introduction

Chapter five of the research gives a summary of the primary discoveries of the study, presenting conclusive remarks and significant suggestions for future actions. This study focused on investigating cybercrime and its impact on economic security within the context of Kenya. The research was motivated by the increasing cyber and online threats to Kenya's economic stability, despite existing measures aimed at safeguarding the Information Communication Technology infrastructure.

5.1 Summary of the Study's findings

The study aimed to assess how cybercrime affects economic security in Kenya, while also investigating the measures taken by the country to address the challenges it encounters in its digital endeavors. To gain a comprehensive understanding of the issues at hand, relevant literature was reviewed based on the research objectives. Regarding the methodology, a mixed approach integrating quantitative and qualitative methods was employed within a survey research framework to facilitate a thorough examination of the subject matter.

The research achieved an 80% response rate, with 35 individuals out of the targeted 50 respondents successfully completing the interview guide. According to the criteria outlined by Borg and Gall (1996), the respondents' return rate can be characterized as outstanding. The researcher took precautions to ensure that a significant majority of participants (17%) had service tenure of 25 to 30 years, while the smallest proportion had served for 1 to 6 years (8%). This approach was

employed to ensure that the participants possessed substantial experience and understanding of the field of study, thereby enhancing the reliability of the gathered data. The implications of extended periods of employment, particularly within the same organization, were also considered.

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

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

The study's findings are consistent with a similar investigation conducted by PWC (2015), highlighting the increasing opportunities and motivations for committing fraud in today's volatile economic environment.

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

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

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

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

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

and the "Budapest Convention on Cybercrime" along with the "Directive on Fighting Cybercrime" from the Council of Europe.

On the contrary, respondents who were undecided indicated that Kenya's cyber space vulnerabilities stem from rapid digitalization without commensurate defense capabilities. The level of cyber risks is directly correlated with the pace of global digitalization growth. These concerns align with the observations of Serianu Consultants in Cyber Security (2015), who noted that institutions addressing cyber-security are lagging behind the rapid advancements in digital technologies.

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

The research highlights the vulnerability of most Kenyans to attacks due to inadequate institutional security measures. It reveals a significant lack of awareness about cyber threats among internet users, enabling criminals to attack without detection. Consequently, both the government and financial institutions suffer substantial losses of funds and valuable information due to this lack of situational awareness. The existing cyber security measures are insufficient to tackle these issues

effectively, as organizations lack the necessary security practices to safeguard critical cyber infrastructure. Therefore, Kenya must reassess its current measures and develop robust national cyber security strategies emphasizing threat management practices to anticipate, detect, respond to, and contain cyber threats.

5.2 Conclusion

This research study concludes that technological advancements have rendered many internet users in Africa susceptible to cyber-attacks, which can originate from anywhere globally. The proliferation of technology has empowered cyber criminals with potent software tools capable of breaching the security of numerous networks worldwide. In Kenya, emerging cyber threats primarily take the form of malware, malicious software that can infiltrate computer systems undetected, including viruses and worms. These threats encompass various forms of attacks such as Botnet attacks, mobile malware, phishing, password sniffing, and Distributed Denial of Service (DDOS) attacks.

The study reveals that of significant concern in Kenya is the widespread lack of awareness among internet users regarding online threats, fuelling the continuous growth of hacker activities. Moreover, institutional involvement in addressing cyber-security issues has been inadequate. However, there is a growing recognition of the pivotal role institutions play in bolstering cyber-security, evidenced by increased investments in the field. Nevertheless, the advancement of information technology has escalated cybercrime, impacting various aspects of modern life, from illegal file sharing to identity theft and online fund embezzlement.

To combat escalating cyber threats, Kenya has embraced internationally recognized standards and forged partnerships with digital stakeholders to develop strategies informed by global cyber-security agendas. The Kenya Computer Incident Response Team/Coordination Centre (KE-CIRT/CC) plays a key advisory role in national cybersecurity matters and incident reporting, albeit facing challenges due to skill shortages and limited resources, jeopardizing its efficacy in the industry.

The study finds that an absence of a dedicated cyber-security regulatory and legal framework in Kenya poses significant risks, as the country grapples with computer-related crimes amidst increasing international connectivity. While Kenya acknowledges frameworks like the Budapest Convention and Commonwealth Model Law on cybercrimes, its existing legislation, such as the Information and Communications Act of 2009, falls short in addressing contemporary cyber-security challenges.

5.3 Recommendations

This study recommends the following in reference to its first objective on the effects of cybercrime on Kenya's economic stability**:**

Cyber Security Education - to address the challenges safeguarding Kenya's economic stability raised in this research, the study recommends the immediate implementation of cyber literacy initiatives, early inclusion of cyber-security education in school curricula, collaborative endeavours among various stakeholders, and the implementation of strong network security protocols. Cyber literacy has become almost must for every individual around the world. More and more the world is becoming interconnected by the internet. The internet has become crucial

for day to day living whether its accessing government services or ordering of goods or services online and even in crucial things like distant learning. Therefore, cyber literacy must make people aware of the dangers that hackers can cause online and what is at stake if their cyber security is compromised.

This study recommends the following in reference to its second objective on the elements of cybercrime as a threat to Kenya's economic security:

Firewall Protection – the study recommends that all government cyber networks and cyber systems be equipped with firewalls and antivirus software to curb the spread of malware in case a network is infected. Employees of organizations that work in an open network must also be made aware of the potential dangers in their cyber space in order to prevent breaches from occurring. But it also helps if individuals or organizations use secure Information Technology products from the first instance.

Based on its third objective on the response mechanism to cybercrime as a threat to Kenya's economic security, the study recommends:

Incorporation of local hackers **-** the study proposes further investigation into the viability of utilizing local hackers to combat cybercrimes, particularly those targeting government databases. These thorough investigations will furnish policymakers, security experts, and stakeholders with valuable insights to develop strategic plans aimed at enhancing Kenya's cyber-security resilience.

5.4 Suggested areas of further studies

This section advocates for further research studies in various areas;

- Cyber challenges across Kenya and the world for the most part is usually asymmetric in nature which means it's done by a small group of people or an individual who are constantly on the move and their targets does not follow a particular pattern. Such attacks have led to breach of government secret records and loss of funds for private institutions, and hence the Government needs to employ the services of local based hackers to combat such menace.

- The growing innovations in online and mobile banking services have exposed customers as well as financial institution to new vulnerabilities. Online and mobile banking attacks are based on misleading the users and silencing login data by using tools such as malware, viruses, warms and Trojan. Moreover, the growth of mobile money technology in the region has attracted criminals to the electronic money transfer platform, and fraudsters are getting clever each day in finding gaps in new security controls implemented by financial institution, organization and individuals.

REFERENCES

Angela G and Martin R. (2012). *Assessing Cyber Threats to Canadian Infrastructure*. Reportprepared for the Canadian Security Intelligence Service, pp. 8-10.

Brenner, S. (2017). *Law in an Era of Smart Technology*, Oxford: Oxford University Press, p. 375.

Broadhurst, R. (2017). *Cyber Terrorism: Research Review*, Australian National University,Cybercrime Observatory, Canberra, DOI, pp. 9-11.

Buzan, B. (1998). *Security: A New Framework for Analysis*, p. 23.

Chatterjee, D. (2019). "*Should Executives Go To Jail For Cyber Security Breaches?*" Journalof Organizational Computing and Electronic Commerce, 29(1), 1–3.

Chuipka, A. (2016). "*The Strategies of Cyber-terrorism*." Graduate School of Public andInternational Affair, University of Ottawa, pp. 4-5.

Communications Authority of Kenya. (2015). First quarter sector statistics report for thefinancial year 2015/2016.

Cyber Security Agency of Singapore. (2016). *Singapore Cybersecurity Strategy*. Retrieved from https://www.csa.gov.sg (accessed 27th August 2024).

Denzin, N. K. (2017). The Research Act: A Theoretical Introduction to Sociological Methods. New York: Aldine.

European Commission. (2020). *General Data Protection Regulation (GDPR)*. Retrieved from https://ec.europa.eu (accessed 27th August 2024).

European Union Agency for Cybersecurity. (2021). *Annual Report 2020*. Retrieved from https://www.enisa.europa.eu (accessed 27th August 2024).

Fischer C. (2006) Research Methods for Psychologists: Introduction through Empirical Studies.

USA, Elsevier Inc.

Gagliardone, I. (2014). M*edia Development with Chinese Characteristics. Global MediaJournal, Government of Kenya. 2014*. Cyber-security Strategy. Ministry of Information Communications and Technology, p. 6.

Kothari, C. (2011). *Research Methodology-Methods and Techniques*, New Age InternationalPublishers, p. 11.

Okongo, C. (2021). "*Evaluating the Challenges and Opportunities of the Use of MilitaryDiplomacy in Intrastate Conflict Management in Horn of Africa*." International Journal of Scientific Research, (2021), p. 2.

Ouma, C. (2021). "*Effective Cyber Incident Response Capacity Framework for CountyGovernment in Kenya: A Case of Migori County*." Department of Computing andInformatics, University of Nairobi," Nairobi, Kenya, pp. 2-4.

Paula, K. (2014). *Kenya Cyber Security Report, 2014*. Nairobi, (2014), p. 91-95.

Possony, S. T. (1946). Atomic power and world order. The Review of Politics, 8(4), pp. 533-535.

Powell, R. (2008). Nuclear deterrence theory: the search for credibility, Digitally printed version. Paperback Re Issue. Cambridge: Cambridge University Press.

Sayigh, Y. (2023). "*Retain, Restructure, or Divest? Policy Options for Egypt's MilitaryEconomy*." Annual Report, Carnegie Middle East Center, Cairo, Egypt, p. 13.

Schelling, T. C. (1980). The strategy of conflict: [with a new preface]. Cambridge,Mass: HarvardUniv. Press.

Sukumar, A and Amoozad, H. (2023). "*Cyber Risk Assessment in Small and Medium-SizedEnterprises: A Multilevel Decision-Making Approach for Small E-Tailors*." WileyPublishers, p. 7.

Statisca, (2024). Internet. Available at https://www.statista.com/statistics/1224168/total-population-of-africa/ (accessed 25th July 2024).

The Government of Kenya. (2014). *Cyber-security Strategy*. Ministry of InformationCommunications and Technology, (2014), p. 76.

The United Nations Office on Drugs and Crime. (2012). *Calculation from Study cyber crimequestionnaire*. Q30 and Symantec. Norton Cybercrime Report, pp. 121-12.

U.S. Cybersecurity and Infrastructure Security Agency. (2023). *Cybersecurity Overview*. Retrieved from https://www.cisa.gov (accessed 27th August 2024).

U.S. Department of Homeland Security. (n.d.). *Cybersecurity and Infrastructure Security Agency*. Retrieved from https://www.dhs.gov/cisa (accessed 27th August 2024).

Zagare, F. C., & Marc Kilgour, D. (2000). Perfect deterrence. Cambridge Studies in InternationalRelations. Cambridge: Cambridge University Press.

Zdzikot, T. (2021). "*Cyberspace and Cyber security*." Springer Link, pp. 29-32.

Ziewitz, M and Brown, I. (2013). *A prehistory of Internet governance*. In Brown, I. ResearchHandbook on Governance of the Internet Cheltenham: Edward Elgar, p. 17.

APPENDICES

Appendix i: Consent Form

Consent Form

My name is …….. I am a student at the National Defence University and National Defence College, pursuing a Master's Degree. It is an academic requirement that data is collected as part of research study.

This interview guide is meant to collect information to examine cyber-crime as threat to economic security in Africa using the case of Kenya. Kindly fill this guide to enable me collect data for this study.

It is my request that you please give a written (signed) consent to be a participant in this study, before beginning. Thank you for taking time to participant in this research, please fill in the guide appropriately, it is my hope that you please answer the interview guide by ticking in the boxes provided as applicable and or writing a brief follow-up statement.

Signed Consent……

Appendix ii: Questionnaire

Serial: .....

Research Interview Guide

This research aims to examine cyber-crime as threat to economic security in Africa using the case of Kenya. The purpose of this interview guide is to collect information from a wide range of informants, who have knowledge about cyber terrorism and national security. It is requested that you please give consent, before you respond. Clarification on each question can be made where necessarily to your satisfaction. The personal information is optional and kindly note that this work is purely for academic purposes only. Please fill in the questionnaire appropriately. This questionnaire will be submitted to you in hard copy.

Instructions

The following statement articulate issues of cyber-crime as threat to economic security in Africa using the case of Kenya. How would you rate some of these statements and give explanations? Where rating scale is 1 = Strongly agree, 2 = Agree, 3 = Un-decided, 4 = Disagree and 5 = Strongly disagree.

Section One: Personal Information

1. Gender? (tick) Male [ ] Female [ ]

2. Age? .....

3. Occupation? .....

4. Office / Ministry / Organization? .....

5. Designation? .....

6. Duration in employment? .....

Section Two: The impact of cybercrime on economic security in Kenya.

Please rate the following statements on impact of cybercrime on economic security in Kenya.

Rating scale: 1 = Strongly agree; 2 = Agree; 3 = Un-decide; 4 = Disagree; 5 = Strongly agree

7. Do you understand the concept of cybercrime? Yes ☐ No ☐

8. Are you familiar with any forms of cybercrime? Yes ☐ No ☐

If yes, which ones?

……..……

……

……

9. How do cybercrime trends manifest?

Explain:

.....

.....

.....

10. In your opinion, is cybercrime well understood in Kenya?

Explain:

.....

.....

.....

11. To what scale does cybercrime affect economic stability in Kenya?

Scale: .....

Explain:

.....

.....

12. Does your organization or institution have a policy that addresses cyber-security?

Explain:

.....

.....

.....

13. Do you think cybercrime has serious implications on the Kenya's national economy?

Explain:

.....

.....

.....

14. Cybercrime has many causes in the Kenyan context?

Scale: .....

Explain: (List some of the causes?)

.....

.....

.....

15. Has the multiagency approach in Kenya been effective in fighting cybercrime?

Explain: (explain by mentioning some of the agencies involved in cybercrime)

.....

.....

.....

16. How often have you experienced cybercrime attacks in your organization?

.....

.....

.....

17. How would you rate strategies and infrastructure for countering cybercrime Kenya today?

Scale: .....

Explain:

.....

.....

.....

18. What strategies do you think are effective to mitigate cybercrime attacks in Kenya?

.....

.....

19. What additional contingency measures do you think need to be put in place by Kenya to fight cyber terror attack?

.....

.....

Additional relevant remarks?

.....

.....

.....

.....

.....

Thank you for your participation.

Appendix iii: Research License

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **372614**

Date of Issue: **18/January/2024**

RESEARCH LICENSE

This is to Certify that Mr.. ISSA CHOCHOTE SAIDI of National Defense University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: "Impact of Cybercrime on Economic Security in Kenya" for the period ending : 18/January/2025.

License No: **NACOSTI/P/24/32603**

372614

Applicant Identification Number

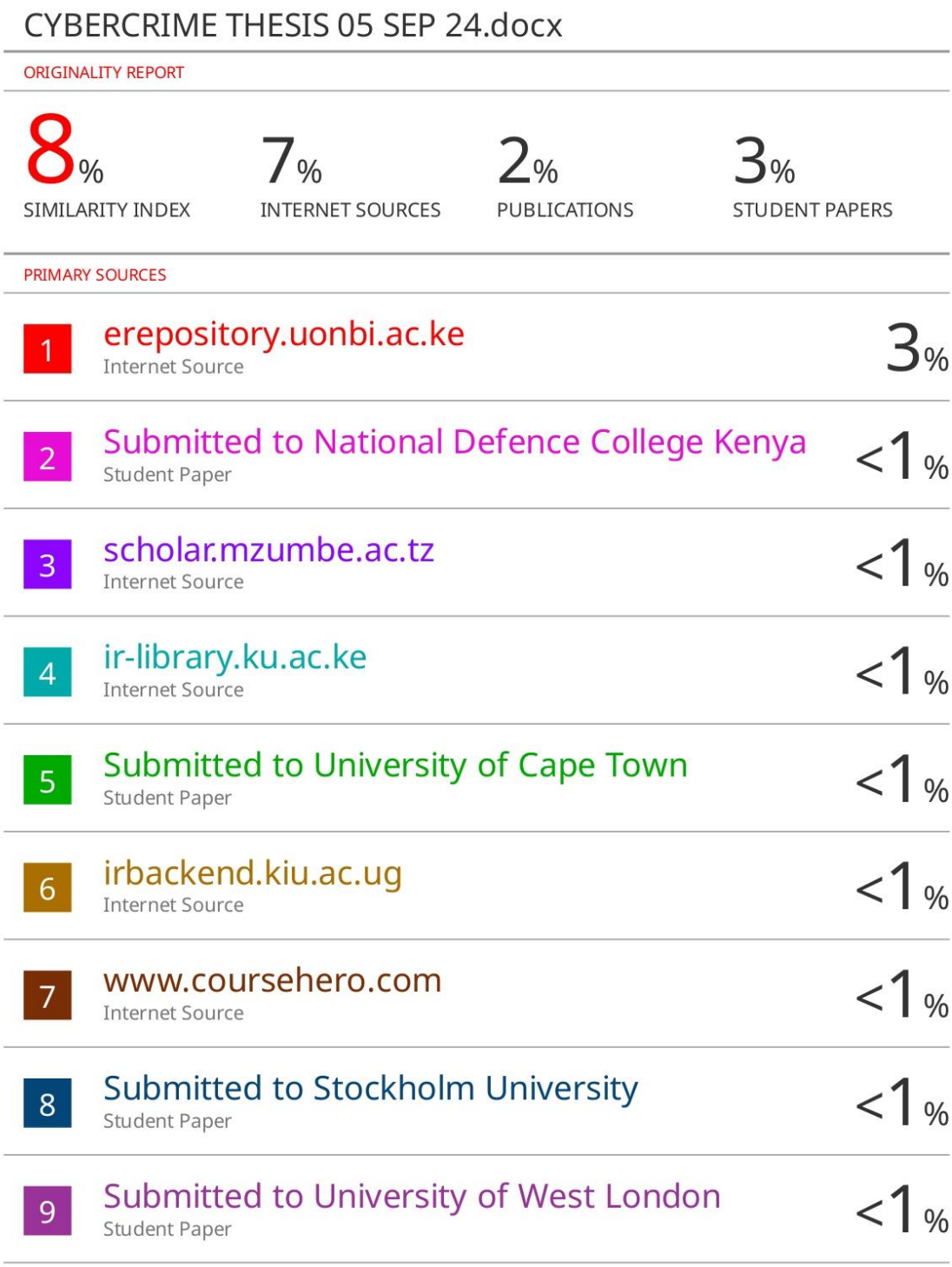
Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

Appendix iv: Similarity Report



CYBERCRIME THESIS 05 SEP 24.docx

ORIGINALITY REPORT

8%	7%	2%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	erepository.uonbi.ac.ke Internet Source	3%
2	Submitted to National Defence College Kenya Student Paper	<1%
3	scholar.mzumbe.ac.tz Internet Source	<1%
4	ir-library.ku.ac.ke Internet Source	<1%
5	Submitted to University of Cape Town Student Paper	<1%
6	irbackend.kiu.ac.ug Internet Source	<1%
7	www.coursehero.com Internet Source	<1%
8	Submitted to Stockholm University Student Paper	<1%
9	Submitted to University of West London Student Paper	<1%