UNIVERSITY OF NAIROBI

INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES

CYBER TECHNOLOGY AND INSECURITY IN AFRICA:

A CASE STUDY OF KENYA

JOSEPH RUTTO KAMARY

REG NO. R/50/9973/2018

RESEARCH SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF MASTERS OF ARTS DEGREE IN STRATEGIC STUDIES AT THE INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES UNIVERSITY OF NAIROBI

OCTOBER, 2018

DECLARATION

I declare that this is my own original work and it has never been presented in any University or Institution for the award of any academic qualification

Signature: _____

Date: _____

JOSEPH RUTTO KAMARY

This thesis has been submitted for review with approval of the University Supervisors

Signature: _____

Date: _____

DR. MUMO NZAU

ACKNOWLEDGEMENT

This thesis would not have been completed without the help, cooperation and contribution of my supervisor, Dr Mumo Nzau, who owing to his long-standing experience as a scholar, guided me through the entire research process. Special acknowledgment goes to all academic and non-academic staff members of National Defence College for the discussions, valuable suggestions and contributions.

TABLE OF CONTENTS

SUBJECT **PAGE**

LIST OF ABBREVIATIONS

AMISOM	African Union Mission in Somalia
AU	African Union
BFID	Banking Fraud Investigations Department
CERT TCC	Tunisian Computer Emergency Response Team Coordination Centre
CIOs	Chief Information Officers
COMESA	Common Market for Eastern and Southern Africa
ICT	Information Communication Technology
IT	Information Technology
ITU	International Telecommunications Union
KE-CIRT/CC	Kenya National Computer Incident Response Team Coordination Centre
KDF	Kenya Defence Forces
M-PESA	Mobile Money Transfer
NIS	National Intelligence Service
NPS	National Police Service
ODPP	Office of the Director of Public Prosecution
TT	Technology Transfer
UK	United Kingdom
UN	United Nations
US	United States
USD	United States Dollar

ABSTRACT

The study explores cyber technology and insecurity nexus in Africa. Africa is rapidly developing in information communication technology (ICT) infrastructure and with this growth more people have been linked to the network. However, this advancement has also introduced key trends to the future of cyber security in the continent. The case study of Kenya was chosen because of the similarities in experiences of cyber security challenges. Securitization Theory was chosen as the theoretical framework in understanding the philosophy behind cyber security measures, with a view to finding an explanation why despite cyber security strategies put in place, the cybercrime incidences continue to be experienced in Kenya.

The study employed qualitative research method and analyzed data obtained from the field including the analysis of secondary data from various academic scholars, journals, publications and other academic works. The study investigated the cyber security strategies and mechanisms available and how they relate to international cyber security regimes. The respondents who participated in this research included professionals in ICT technical roles, ICT security officers, academia, IT institutions and others. This research explored the measures and strategies applied in Kenya to safeguard the ICT sector against cyber threats. The measures include developing cyber capacity and national institutions to provide a secure and safe cyber environment.

The study analyzed how cyber technology has impacted on Kenya's national security. The research contextualized the concept of cyber security within the Securitization Theory context in order to appreciate cyber technology and its effects to national security. The highlight is on how cyber-attacks in Kenya have become prevalent and its porous nature and complexity. The increase has been associated with the use of computers across the public and private sectors which has attracted criminals to exploit the opportunities available. As outlined in the trends of threats presented, the attacks have become increasingly sophisticated because of the asymmetric nature of operations. This provides a basis through which to evaluate Kenya's cyber security position.

The study therefore concludes that there is a strong correlation between the growth in technology and in-security. The study proves that legal frameworks that provide for cyber security do exist. However, the area of weakness is in implementation due to weak structures and lack of enforcement mechanisms. The country's cyber position therefore remained weak because of lack of cyber threat awareness amongst many internet users. However, there was a growing acknowledgement of the important role played by institutions through investing in cyber security as a major step towards enhancing cyber threat capacity. Finally, the research also provides recommendations on measures that can achieve sustainable cyber security which must be anchored on cooperation of all stakeholders including internet users and researchers.

MAP OF STUDY AREA I

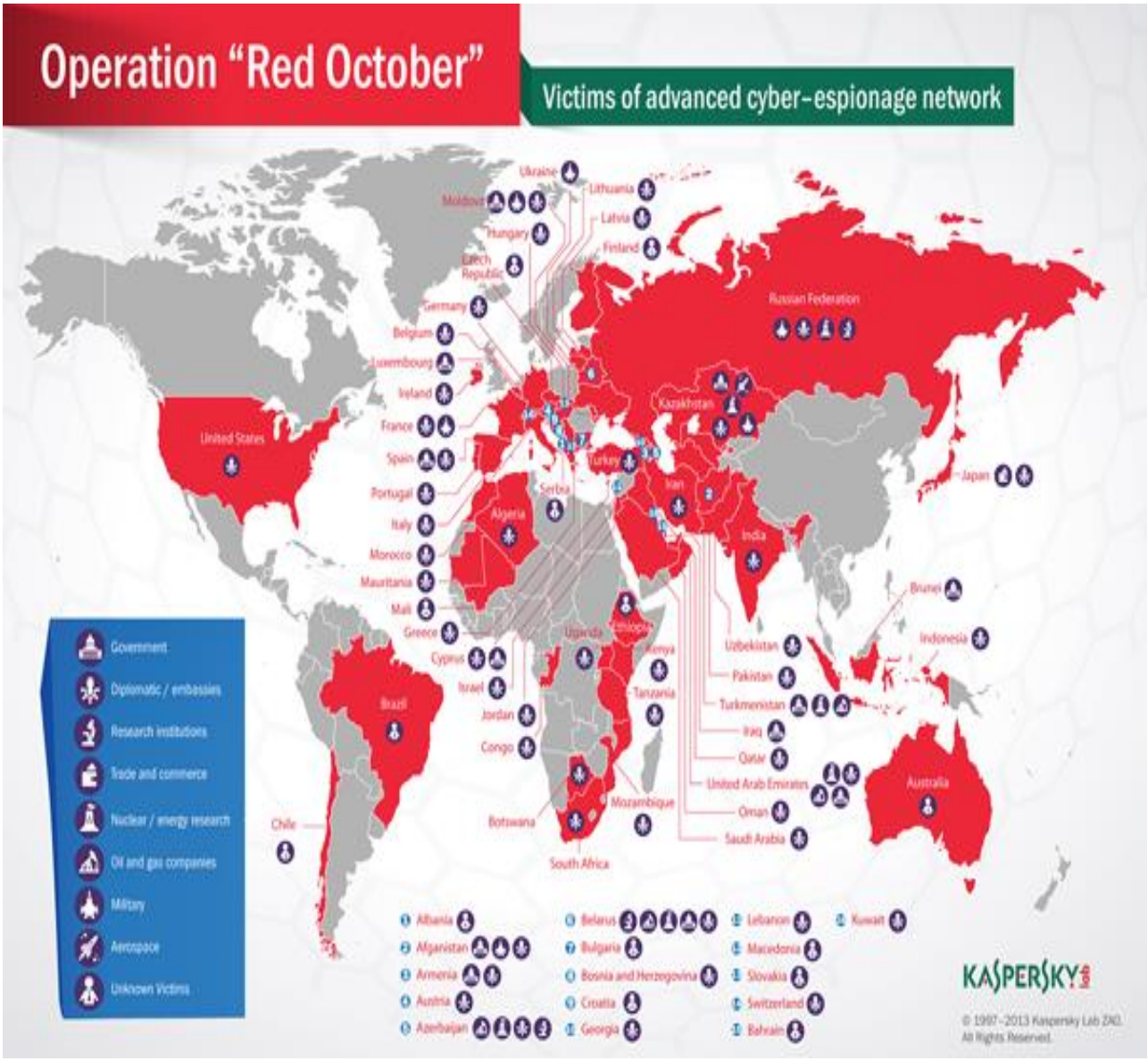


Figure 1: Technology hubs in Africa

Source: United Nations. 12th UN Congress and Crime Prevention and Criminal Justice (2010)

MAP OF STUDY AREA II

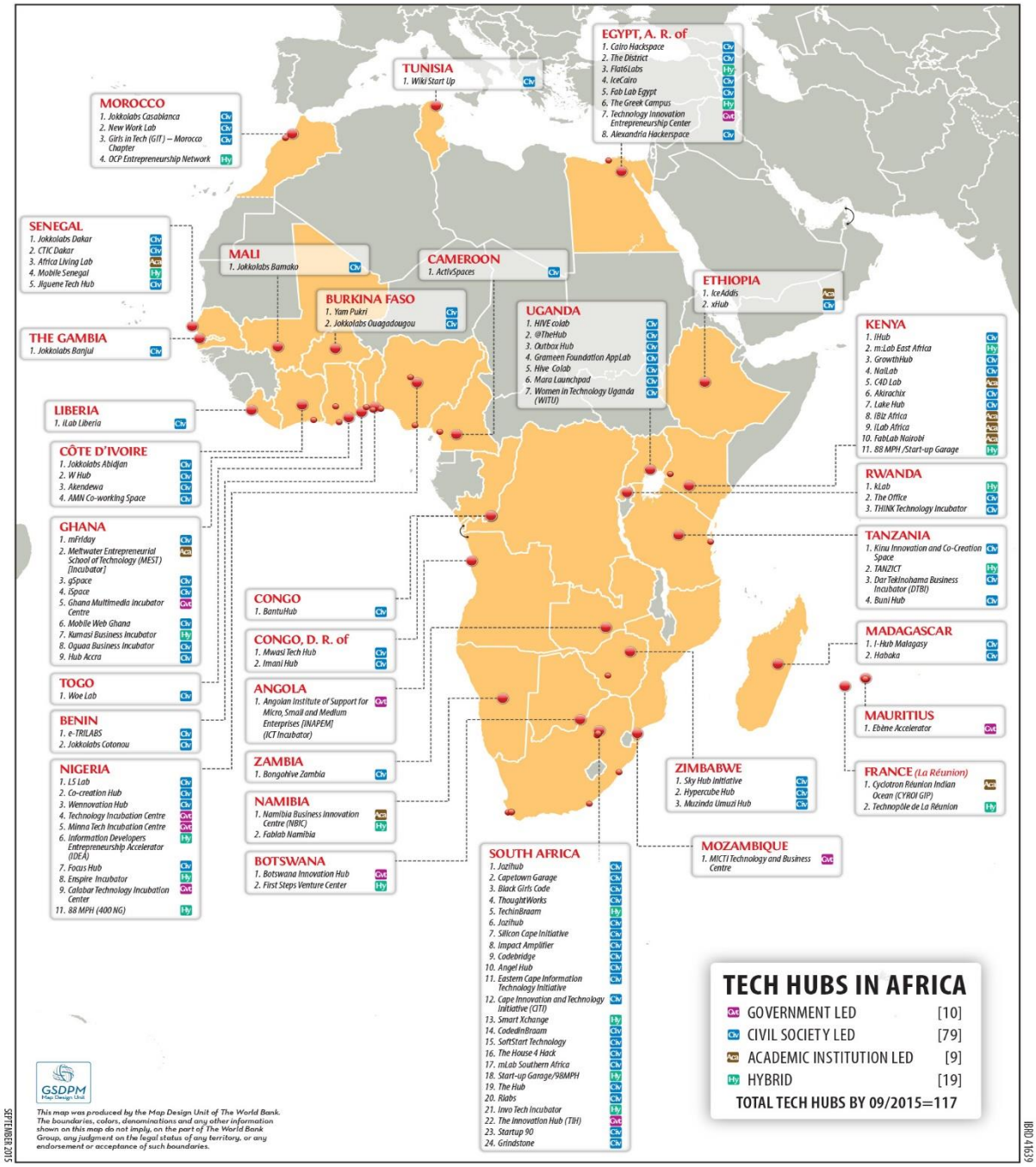


Figure 2: Technology hubs in Africa

Source: Convention of Cybercrime. The Convention of Cybercrime, a Unique Instrument for Intl Co-operation, (2001)

MAP OF STUDY AREA III

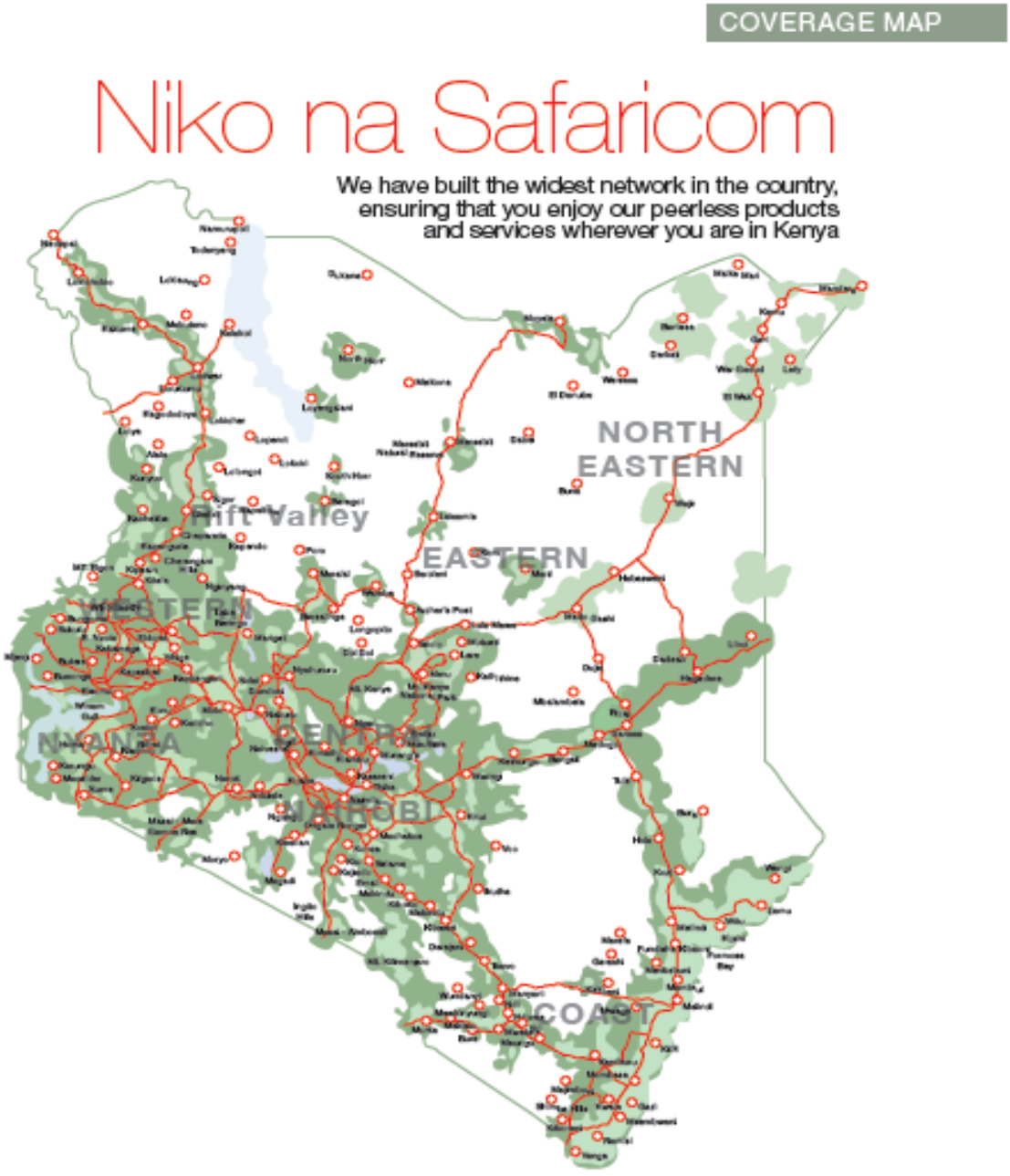


Figure 3: Mobile phone coverage in Kenya

Source: Google (2017)

CHAPTER ONE

INTRODUCTION OF THE STUDY

1.0 Introduction

Africa is a continent with enormous natural resources and economic diversity, but remains underdeveloped.[1] In the past decades, Africa has experienced high and growing economic development that has driven experts to argue that the Africa is at a turning point with respect to its developmental and technological agenda ready to become a key participant in the international economy. 21st century particularly will be recalled for fast paced cyber technology as an emerging security challenge in the modern world. With the coming in of the age of information and introduction of digital enabled technology network, has expanded the space of interaction in governments, security services, business and personal level, because of accessibility to information. The Internet technology in Africa forms part of a significant component of cyberspace technology system which has had a lot of influence in many livelihoods.[2] However, as the continent and the world is busy exploring the importance of digital technology, the network infrastructure is increasingly being exposed to severe threats. The rising fear of cybercrime has tended to exploit digital platform and space posing a serious security threat.[3]

Despite this exponentially rising significance, there have been no overarching and widely agreed methods of addressing the threats. While most states are trying to develop national measures and legislation on cyber security, they have not been able to find absolute solutions to the threats. Nonetheless, there has been no universally agreed framework to deal with cyber threats except

[1] GPF, *Global Policy Forum*, 2014, p. 1: Available: https://neu.globalpolicy.org/sites/default/files/download/jahresbericht/GPF_Annual_Report_2014_web.pdf.
[2] Akubue, A. Appropriate Technology for Socioeconomic Development in Third World Counties. The Journal of Technology Studies 26 (2000), pp33-43.
[3] ETC (Action Group on Erosion, Technology and Concentration). The Big Down: Technologies Converging at the Nano Scale. Ottawa: ETC Group, (2003), p. 89.

legislations by individual governments, which most of their efforts have not fully provided cyber security as they are limited by application.[4]

1.1 Background Information

The continent of Africa is on the rise with high growth in economy, population and international influence, (Moeng, 2011).[5] The continent has a population of about 1.5 billion people with a median age of 20 years, which is regarded as the youngest population in the world. With its prominence of the youthful population comes the urge for productive employment and increased social engagement including global connectivity. The capacity to innovate and adapt new technologies has enhanced their chances of competing effectively in the global market scene. However, Africa is known to be a continent that has not adopted the technological advancement and this gap has remained to be a source of rising economic and security challenges.[6]

In the new world order, development is understood in terms of economic and technical advancement and the capacity of a nation to attain the ability to exploit the opportunities presented in order to achieve higher standards of economic wellbeing of its people. Developed countries have sustainable ability to use science and technology to draw out economic dividends from the environment. Technology is used to transform natural resource from the environment into objects to consume, sell, use for as part of a process to produce other economic goods.[7]

On the other hand, developing countries such as Africa are least developed in science and

[4] Ploch, L. 2010. "Countering Terrorism in East Africa: The U.S. Response. "CRS Report for Congress, Congressional: Research Service.
[5] Moeng, B. Reasons to invest in Africa ICT. IT News Africa, (2011), p.17.
[6] Herbert Lin, 'Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion,' Georgetown Journal of International Affairs, Special Issue, International Engagement on Cyber. Establishing International Norms and Improved Cybersecurity, 2011,pp.127-135.
[7] Odedra, M. 1990a. Information technology transfer to developing countries: It is really taking place? Paper presented at the Conference on Information Technology Assessment. 9-12 July. University of Dublin, Dublin.

technology and therefore are not able to exploit their environment for economic goods. The continent has therefore depended on the developed nations of the West for the provision of technology of their industrial development. Consequently, Africa has remained with the least functional level of infrastructure such as electricity, telecommunication and transportation. The continent finds it difficult to close the technology gap with the West.[8]

There are many reasons given for African's inability to acquire modern technology. It was initially believed that buying technologies from the West would cause technology transfer to take place, and that having Western Companies and Multinationals Corporations (MNC) set up companies in the continent would automatically bring about a transfer of technology. Unfortunately, all of this did not result in the desired state of technology transfer because the MNC do not want to part with their proprietary technology, which they regard as giving them competitive position in the world market.[9]

Cyber technology is the new age of Information Technology (IT) which includes electronically processed information and knowledge as a resource for nations and organizations.[10] The computer systems have allowed states, institutions and individuals to collect, store and communicate massive information and data in a wider geographical landscape. The ability to harness information and knowledge underline the success of using technology in all domains. Cyber technology is now widely used as a precious resource with which to enhance and maintain a competitive position in business across the whole world.[11] As a result of cyber technology systems that can capture and utilize human expertise, business organizations are now able to use this knowledge as a resource and strength in their quest for market control and competitive power.

[8] Cole, S.1986. The global impact of information technology. World Development, Vol.14,no.10/11.
[9] Bessant, J. 1984.'Information Technology and the North-South Divide.' In new information Technology, edited by A.Burns. West Sussex: Ellis Harwood.
[10] Bayart, J.-F.2000. "Africa in the world: A History of Extraversion." African Affairs 99 (395): 201-67.
[11] International Strategy for cyberspace- Prosperity, Security and Openness in Networked Word', The White House, May 2011, available at www.whitehouse.gov/sites/default/files/rss_viewer/international_for_ cyberspace.pdf. All internet references were accessed in September 2012, unless otherwise stated. Accessed on 13 September, 2017

The potential and possibilities offered by Information Communication Technology (ICT), lead to its examination with reference to Africa and how theses technology has affected business and security.[12] There has been a lot of scholarly work to show how ICT is vital for the survival of most businesses, organizations and states today. States trying to exist today without a major examination, utilization, development and active application of cyber technology have suffered the consequence. However, those states, organization and individuals who control the sources of IT have gained an age or power over their societies and environment. Hence effective use and application of technology have led to individual, economic and security wellbeing of a state.[13]

Africa can therefore not afford to miss this technology revolution to pass by them. The modern ICT systems have brought about the means of improving the management of organizations in terms of planning, production and service delivery in all areas of the economy. The ICT acceptance continues to raise together with mobile devise rights increasing exponentially while social media application and internet quickly becoming a reality.[14] MacAfee argues that Africa has a huge growing number of cell phones and internet users across the continent.[15] This metric shows that the continent is poised to gain and assist to enhance global development. A long with this growth in the economy, the emergence of e-commerce industry is equally expanding and is expected to reach about $75 billion USD by the year 2025. This growth in digitalization gives rise to a new risk and vulnerabilities that is likely to weaken progress, (Brenner (2007).[16]

The expansion of internet utilization and growth in cyber technology has presented both prospects to business as well as crime rates. The growth in technology and online communication has

[12] Akindale, T. 1986. Computer as a tool for national development: Getting started. Informational Technology for Development, vol1 No.3 September.
[13] Bhatnagar, S.C., ED. 1992. Information Technology Manpower: Key issues for Developing Countries. New Delhi: Tata McGraw-Hill.
[14] Internet World Stat, (2017).
[15] MacAfee 2014, MacFee Labs Threats Reports. Internet www.macfee.com/hk/raesources//reports/rp-quarterly-threats-ql-2015. Accessed on 20 May, 2017
[16] Brenner, S.Law in an Era of Smart Technology, Oxford University Press, (2007),p.375.

led to the new wave of insecurity.[17] Consequently, cyber threat is asymmetric in nature including its actors. The growing incidences of criminal events and the likely intensification of a variety of new illegal activities pose a challenge on legal systems and security agents (Brenner, 2007).[18]

A growing number of cyber securities are taking place in most African counties.[19] Cyber threat is emerging as a new form of warfare, spreading its effects across boundaries. The attacks are becoming a lucrative activity perpetuated by the enemies of states, (Hold Security Report, 2014).[20] Cyber threats have found open space in the overreliance on internet infrastructures which has been used to target government institutions, industries, business and security agents throughout the world, (Lawrence Gershwin, 2001).[21] 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. These include anonymous calls, banking frauds, espionage, web defacement of government sites and other service interruptions. Breaking into computer system is because the criminals are able to access it due to the open space of operations and the motivations available, (Hollis and Post, 2010).[22]

Regrettably, these incidents have exposed African leadership preparedness to inadequately address the problem. This scenario has obligated most governments to respond through legislation, however, the laws and measures remain a challenge to enforce. Consequently, several steps are still required to make these laws enforceable by penal procedures and law enforcers' competence. The lack of adequate cyberspace security strategy means that Africa will remain vulnerable to the cyber technology criminals, (Ranz-Stefan, 2010).[23] These weaknesses can be explained along lack of

[17] Longer O.B, and Chiemeke S. C. Cybercrime and criminality in Nigeria – What roles are internet access points in playing? Eur. J. Soc. Sci 6(2008), pp.133-139.
[18] Brenner, S. Law in an Era of Smart Technology, Oxford: Oxford University Press, (2007), p.375.
[19] Symantec Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18(2013), p.79.
[20] Hold Security. You Have Been Hacked! Internet//http//www.holdsecurity.com/news/cybervor-breach, (2012), p. 77.
[21] Lawrence, G Cyber Threat Trends and U.S. Network Security, Statement for the Record to the Joint Economic Committee National Intelligence Council, (2001), p. 16.
[22] Duncun, B.H. and David, G P. Do Cyber-Attacks Require a Duty to Assist? Law Technology News, (2010).
[23] Ranz-Stefan, Gacy, foreign policy: Africa's internet threat, National Public Radio, (2010),p. 23.

competence in leadership to seize the potentials that the technology offers and the risks posed owing to the lack of strategy to guarantee safe growth of cyberspace.

As we note, the existing cyber security measures are regarded as passive in nature and thus fail to transversely address the challenges, (Abraham, 2010).[24] Despite the multifaceted approach put in place in combating cyber threats in Africa by various players in economy and security sectors, little information is available on Kenya's preparedness to face the nascent nemesis. This reality still remains constant today and it is for these reasons that the study aims to analyze how cyber technology affect security in Africa, using a case study of Kenya.

1.2 Problem Statement

The primary responsibility of any state is the provision of security to its citizens, economy and institutions amongst others, (Collins, 2013).[25] Whereas, states have found it easy to manage national security within their defined borders, they have incurred challenges evolving from advancement in technology, (Brauch *et al.*, 2011).[26] Kenya faces the challenge of emerging threats to national security emanating from the widespread utilization of cyber technology. For example, cyber technology has been used to break into government networks, financial institutions and security offices to gain access to information.

Kenya, in respect to the challenges has put in place intervention measures, the problem still persists with dire consequences. The intervention measures appear to be ineffective to stop cyber-attacks. If the problem is not adequately addressed, its management will be complex to handle in future.

[24] Abraham, D. The Best Defense? Legitimacy and Preventive Force, Stanford, CA: Hoover Institution Press, (2010), pp. 32-35.
[25] Collins, A. Contemporary Security Studies, (UK: OUP, 2013), 9.
[26] Brauch, P, I, et al. (eds.), Coping with Global Environmental Change, Disasters and Security, Hexagon Series on Human and Environmental Security and Peace 5, Springer- Verlag Berlin Heidelberg, (2011), p.87.

This study will therefore seek to identify security challenges facing Kenya in the use of cyber technology and the remedies that may be deployed to solve it.

1.3.1 General Objective

To investigate the contribution of cyber technology to In-security in Africa

1.3.2 Specific Objectives

1. To examine the cyber technology - (in) security nexus in Africa.
2. To assess the emergent patterns of cyber technology as a national security threat in Kenya.
3. To evaluate cyber security measures and strategies applied in Kenya.

1.3.3 Research Questions

a. What are the factors in cyber technology that contribute to economic development and insecurity?

b. What is the nexus between cyber technology and In-security?

c. How effective are the existing measures and strategies to address cyber security in Africa?

1.4 Hypotheses

The research will focus on the following hypothesis:

a. Cyber security is influenced by the advancing technology in ICT.

b. Cyber intervention measures and strategies are ineffective against cyber threats in Kenya.

1.5 Academic Justification

The threat posed by cyber technology on national security has become a major global discourse in recent times. Many countries have fallen victims of cybercrime with huge losses of personal data, finances, government secret information and others. Due to the tangible effects of cybercrime, a lot of scholarly attention has been directed towards associated impact. While there is abundant literature on the phenomenon of cyber threats and its related consequences, it is however, noted that there is limited study on the technology in-security nexus. As such there is information gap in this respect. This study will hence form part of the necessary step towards the generation of knowledge that would help in understanding the link between cyber technology and its role in national security. The study will also evaluate why measures and strategies developed are responding to technology in-security challenges.

1.6 Policy Justification

This study notes that cyber-incidents in Kenya have caused significant damage. Kenya has lately been a victim of international cybercrime with the most recent one in 2017 involving criminals from China, America and Europe, the Government has developed measures to strengthen the cyber security strategies to deter the threats in the country.[27] Among the steps taken include the establishment of Cyber Security Strategy Plan 2017/18, Cyber Security Policy 2016, Cyber Crime Bill 2016 and Cyber Misuse and Cybercrimes Bill 2018.[28] These efforts also include the establishment of Cybercrime Police Unit to deal with offences relating to computer systems, including online insults, wrongful distribution of obscene images, cyber terrorism and espionage. All these strategies are aimed at deterring cybercrime. However, civisms of their ineffectiveness have been noticed demonstrating a lacuna between the cyber security and the measures put in place to address the nascent crimes. It can also be observed that most

[27] Nzwili, F.2015. "China Kenya at odds over suspect Chinese Cybercriminals." The Christian Science Monitor. Available at www.csmonitor.com/World/Africa/2015. Accessed 08 September, 2018.
[28] Daily Nation, Thursday 17, 2018.

internet users both at individual and institutional level have very little understanding of the cyber legal framework that are supposed to protect them.

The research is thus expected to provoke national debate and inspire policy formulation for the establishment of strategies and programs to better enhance cyber awareness amongst the users. Further, the findings of this research will help in mobilizing national efforts in identifying emerging trends and patterns of cyber technology that present a threat to the national security. Through these study policy makers will identify the gaps in the current cyber security systems and propose remedial measures that will ensure better and effective mechanisms for managing and mitigating cyber threats.

1.7 Scope and limitations of the Study

The focus of the research is on the influence that cyber technology has on security in Africa, a case of Kenya. This study will be limited to investigate emerging trends and patterns of cyber technology and there impacts on security in Kenya. The focus population will comprise key stakeholders in Kenya ICT industry drawn from both public and private sectors.

The main limitation likely to be faced is that a few of the targeted respondents may consider some of the information sought as being sensitive and will not reveal their strategies to competitors. This limitation will be managed by making clarifications and assurances that the aim of the research will be for academic purpose and not any other interests at all. Since few similar studies have been done in the subject especially in Africa and Kenya, there will limited empirical literature on the area of cyber technology and its implications in security in Kenya. This limitation will be minimized by exploring similar studies done in other geographical areas while maintaining focus on the primary variables of the study.

1.8 Literature Review

The purpose of this literature examination is to present context to the study of works of scholars in the area of cyber technology and implications to national security. The literature review is based on objectives of the study definitions and an outline of cyber technology and implications to security in Africa and around the world. Building on the writings of scholars on cyber security and the nexus with technology, the research will provide an outline of how the continent has responded to such threats while developing the ICT infrastructure to support economic growth, (Davis & Pease 2000).[29]

Africa is comparatively referred to be a newcomer in the world of internet usage. Cyber security has emerged to be a major threat facing contemporary societies and when it comes to the continent, the challenge is even worse. Africa is facing a barrage of internet related threats concerning security risks, intellectual property rights and protection of personal data.[30] A study by International Data Group Connect, examining the status of threats of cyber in Africa with focus in Kenya, Nigeria, South Africa and Egypt, indicated that there exists a strong correlation between economic development and cyber technology.[31] The study therefore acknowledges that growth in technology predisposes new challenges and vulnerabilities.[32]

The existing academic and policy associated literature on the cyber technology and in-security begins by outlining the growth of information technology age and the emergent challenges. The existing scenarios on digital divide shows remarkable difference amongst developed and countries that are developing such as Africa and Asia in respect to security preparedness due to rising global demands and

[29]Davis R & Peace K 2000. Crime, Technology and the future. Security journal 13(2):59
[30] Sheldon, J., 2013. The Rise of Cyber power. In: Strategy in the contemporary world. New York: Oxford University Press.
[31] International Data Group Connect, Africa 2013. "Cybercrime, hacking and malware." White paper. Available www.idgconnect.com/view_abstact/1140/africa 2013. Accessed 15 Aug 18
[32]Symantec Corporation, 2016 Norton Cybercrime Report, September, 2016.

the security measures in place.[33] Additional risk linked to globalization is the increased trends in technology related crimes emanating from regions with less enforcement such as Asia and Eastern Europe.[34] Most developed countries of the West suffer from cyber technology attacks because of lack of harmonized laws and disparities between them will continue to pose a challenge.

According to Colwill, the growing adoption of internet technology as a communication platform and the predisposition of service providers to invest in developing countries such as Africa where labor costs are cheaper, will continue to present a challenge, (Colwill (2007).[35] The societal overreliance on information system is overwhelming with most activities depending on network enabled capacity, (Ganuza, 2011:11).[36] Among the key threats is attack targeting a range of critical infrastructure resources, for example telecommunication, security sector, government departments, financial services and other sectors of the economy.

In most security literatures, cyber security is used as a collective term which is a subject of international interest as well as importance.[37] The definition of the term cyber security varies, for example according to Merriam Webster dictionary, the term refers to actions taken to protect a computer system against an authorized access or attack. While ITU defines cyber security as an identification of policies and measures taken to safeguard the cyber infrastructure and environment.[38] Organizations and owner assets include linked computing devises, computer appliances, telecommunication systems and information storage in cyber environment.

[33] Arbon Networks 2006. Worldwide infrastructure security report.
[34] Singer, P. & Friedman, A., 2014. Cyber war: What everyone needs to know, New York: Oxford University Press
[35] Colwill C% Gray A 2007. Greeting an effective security risk model for outsourcing decisions. BT technology journal 25(1):79-87
[36] Ganuza, N., Hernandez, A. and Benaventa, D. (2011) "An Introductory Study to Cyber Security in NEC" NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia.
[37] Klimburg A, Editor. National Cyber Security Framework Manual. NATO.CCD COE Publishers, 2012.
[38] International Telecommunication Union. ITU-TX.1205: series x: open system communication and security: overview of cyber security, 2008.

The term cyber security and information security have been used interchangeably. Whereas, they are comparable, the two concepts are not totally similar.[39] The information security is a term applied to ensure business continuity and minimize the impact of security incidences to the business unit. While communication technology security is concerned with aspects of safety of systems based technology where information is normally kept. This supposes that there exists a distinction concerning safeguarding an information resource and communication technology infrastructure.[40]

When analyzing ICT security, as confirmed in the above argument, cyber security therefore be used to denote the protection of appliances that are of common interest to society that include significant national infrastructure. This implies that cyber security includes anything that is accessed through the cyberspace. The term cyber security can therefore be assumed that it is correlated to information security, but not similar. However, in cyber security ICT and information are the fundamental sources of security weaknesses.[41]

Cyber security therefore is understood to emanate from cybercrime which result from information and ICT security weaknesses. The concept of cyber based crime does not differ much to the understanding of the conventional crime as the two cover the conduct or action, that lead to breaches of a national security.[42] The present meaning of cybercrime has evolved and tends to vary according to the perception of the observer, victim or protector agents. According to the Council of European Cybercrime Treaty, they define "Cybercrime" as an offence that cover criminal activities against information and ICT. However, Zeviar-Geese (1998), disagree with this definition and potent that it must be widened to include activities such as cyber-stalking, fraud, access to unauthorized information

[39] Whitman ME. Mattord HJ. Principles of Information security 3rd ad. Thampson Course Technology; 2009.
[40] Wood CC. why information security is now multi-disciplinary in nature, multi-department, and multi-organizational in nature. Computer Fraud & Security 2004;2004(1):16-7
[41] Rossouw Von Solms, Johan van Niekerk. "From Information Security to Cyber Security", Computer & Security. 2013
[42] Kuehl, D., 2009. Cyberspace and Cyberpowe. In: F. Kramer,S. Starr & L. Wents, eds. Cyber power and National Security. Dulles: Potomac Books, p.28

and child pornography.[43] Similarly, Shinder (2002), considers cybercrime as a subset of computer crime which refers to unlawful offenses committed by means of the internet or other computer system applications (Shinder, 2002).[44]

Mallory, (2007),[45] on the other hand expanded this definition and argued that cybercrime is a crime associated with internet technology which concerns citizens, governments and industries where crime manifests in many forms such as cyber stalking, phishing (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 phases of computer use are vulnerable to criminal action both as a target or agent of fraud.[46] The predominant types of computer frauds include indefinable computer resources represented in data form such as financial transactions which are lucrative targets of fraud related to computer. In modern business environment most, financial transactions are processed through computer systems by use of credit cards and other electronic devices which have become potential grounds operating for organized criminals, (Siegel, Saukko, and Knupfer, 2000).[47] Clearly, the internet technology has produced an atmosphere which offers opportunities for criminal events which translates to threats to state security.

Just recently, cyber security has grown from a concern to threat to an issue of urgent importance to the future of Africa.[48] The increasing awareness of cyber-security threats in the continent, has elicited old clichés regarding the existing gaps between Africa and more advanced countries of the West.[49] The

[43] Zeviar, G. The State of the Law on Cyber jurisdiction and Cybercrime on the Internet, California Pacific School of Law, Gonzaga Journal of International Law, vol. 1, (1998), p.219.
[44] Shinder, E.2Ed Scene of the Cybercrime: ISBN: 978-1-5949-27608, (2002), P.89.
[45] Mallory, S. L. Understanding Organized Crime, Jones and Bartlett, (2007), pp. 10-12.
[46] Herbert Lin, 'Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion,' in Georgetown Journal of International Affairs, special Issues, International Engagement on Cyber. Establishing International Norms and Improved Cybersecurity, 2011, pp. 127-135.
[47] Siegel, J. A., Saukko, P. J. and Knupfer, G. C. Encyclopedia of Forensic Sciences, Academic Press, (2000), p.67.
[48] Quarshie, H. O. and A. Martin-Odoom. 2012. "Fighting Cybercrime in Africa. "Computer Science and Engineering 2(6):98-100.
[49] ITU. 2015. ICT Statistics. Available www.itu.int.en/ITU-D/Statistics/Pages/stat/default.aspx. Accessed on 30 September 2017.

literature available about Africa cyber security has been informed by exaggerated tones, portraying Africa as a safe haven for cybercriminals, (Kharouni 2013).[50] However, there is no explanation to support the argument that Africa has become unsafe continents to live in, safe for their sponsored narratives on Africa cyber security which have been observed to be biased, (Jackson 2015).[51]

This study, while recognizing the challenges facing cyber security in Africa and contradictions relating to the measures introduced endeavors to explore the specific weaknesses on the distinctive digital cultures of the continent.[52] The continent has experienced faster growth in Mobile phone banking innovations which have led to loses and increased chances of theft in the business (Harris, Goodman and Traynor 2013; Herbling 2014).[53] Electronic financial transactions have become a safe haven for insider theft in the banking organizations has given space for these transfers by criminals, (Mukinda 2014; Quarshie 2012).[54] The continent's thriving economy has undeniable link to the success of the cyber technology, (Moeng, 2011).[55] This has been achieved by the freedom and independence in the sector where both corporate and individuals competes freely in the market. This number has attracted international investors into the continent wishing to reap from the market opportunities presented.

The study by J. O'S (2013) on the African economic index lends rich idea to the current study by showing how ICT is important in the growth of the economy.[56] However, a closer look at the structure of internet use in the continent and its correlation with economic expansion and prosperity reveals a little

[50] Kharouni, L.2013. "Africa: A new safe harbor for criminals" Trend Micro Incorporated Research Paper. Available at www.trendimicro.co.uk/media/misc/africa new-safe-harbour for cybercriminals. Accessed 07 September, 2018.
[51] Jackson, T.2015. "Can Africa Fight Cybercrime and Preserve human rights" BBC News. Available at www.bbc.com/news/bussiness. Accessed 12 August 2018.
[52] Kharouni, L. 2013. "Africa: A New Safe Harbor for Cybercriminals:" Trend Micro Incorporated Research Paper. Available www.trendmicro.co.uk/media/misc/africa-new-safe-harbon-for-cybercriminals-en.pdf. Accessed on 30 March 2018
[53] Harris, A., S. Goodman and P. Traynor. 2013. Privacy and Security Concerns with Mobile Money Application in Africa." Washington Journal of Law, Technology and Arts 8(3): 245-64.
[54] Mukinda, F.2014. "Fraudsters find Easy Cash in Mobile Banking, Report says." Daily Nation September 2015. Available www.mobile.nation.co.ke Accessed 25 June, 2017.
[55] Moeng, B. Reasons to invest in Africa ICT.IT News Africa 14, (2017).
[56] J. O'S. " Growth and other good things", The Economist, May 2013. Available at www.economist.com/blogs/boabab/2013/05/development-Africa. Accessed 15 Aug 18.

surprise. There is a large inconsistency in the level of penetration of internet technology. According to the Internet penetration report of 2016, Mali, Malawi and Madagascar are among African countries with the highest penetration of an average of 72.5%. While Ethiopia is rated the lowest, the penetration remains at only 1.9%. But Mali, Malawi and Madagascar with 2015 Gross Domestic Product (GDP) per capita of $1,559, $781 and $1,429 respectively, are not among the richest countries in Africa as compared with Ethiopia whose GDP per capita is $1,533. Clearly, there is no visible correlation with GDP per capita or economic growth; nevertheless, modernization of economies has a relationship with internet technology.[57]

With the increasing technology, comes cyber security concern. Cyber security is a growing concern for African organizations as technology evolves, so is the nature and prevalence of cyber threats.[58] Cyber security if not well addressed, is likely to reduce considerably the benefits that Africa has gained over the years from ICT advances. The United Nation realizing that Africa and other developing counties were affected by cyber security, adopt a resolution in 2002, which mandated the ITU to assist the continent develop capacity in information technology in order to help them adapt appropriate measures on cyber security.[59]

Equally, "the African Union Convention on Cyber Security and Personal Data Protection", in 2014 added its weight to improve cyber preparedness in the continent, (Access 2014).[60] Africa today is facing difficulties keeping up with new actors and technologies arising from transnational threats like terrorism and now cyber security, (Macharia 2014).[61] The continent is finding it a challenge to control

[57] A 2011 Deloitte Touche Survey.
[58] MacAfee 2014, MacAfee Labs Threats Reports. Available Internethttp//www.macfee.com/hk/resources//reports/rp-quarterly-threats-q102015.Accessed on 20 August 2017
[59] ITU.2015.ICT Statistics. Available www.itu.int.en/ITU-U/Statistics/pages/stat/default.aspx. Accessed on September 2017.
[60] Access.2014. "African Union Adopt Framework on Cyber security and Data Protection" Available at www.access-adopt-framework.org/blog/2014/african union adopt framework on cyber security and Data Protection. Accessed 10 August, 2017.
[61] Macharia, K. 2014. "Africa Needs a Cybersecurity Law but AU proposal is flawed. Available at www.techpresident.com/news/wegove/africanunion-cybersecurity -law-flawed. Accessed 05 September, 2018.

new generation of global issues together with what takes place within its borders. According to Gluckman J (2011) on the study, "Improving the Transition Reducing Social and Psychological Morbidity During Adolescence Wellington," argues that while rapid technological development have provided vast areas of new business opportunities, the new technologies have also resulted to a security dilemma.[62]

On cyber security, states have been affected by private actors who control the operations of cyberspace infrastructure.[63] Gluckman and Ribabu on their studies contribute hugely to the field of cyber technology and insecurity in Africa which is the current field of study.[64] They observed that many organizations both public and private have experienced breaches of cyber security. This is a gap that the study strives to fill by identifying factors that has led to cyber insecurity in Kenya. This study notes that since the year 2000, ICT was identified as a major driver to Kenya's economy. Since then, Kenya has witnessed increased use of internet which stands at 40 million and 90 percent penetration as at 2016.[65] The fast growth of ICT in innovative technologies shows how Kenya has become independent to the sector, (CAK, 2016).[66]

The first case of international cybercrime in Kenya in 2014 uncovered some of the cyber weaknesses in the national cyber security preparedness.[67] The Kenya Information Technology, Security and Association (ISCA) confirmed the incident which uncovered the weaknesses of the Kenya cyber space.[68] As noted by CAK, the existing cyber security measures are generally passive in nature and thus

[62] Gluckman, John 2011. Improving the Transition Reducing Social and Psychological Morbidity During Adolescence (Wellington, Office of the Prime Minister's Advisor Committee, 2011), p 24
[63] Bayart, J.F.2000. "Africa in the world: A history of Extraversion." African Affairs 99(395):217-67
[64] Ribadu, E. (2207), Cyber Crime and Commercial Fraud: A Nigerian Perspective. A paper presented at the Modern Law for Global Commerce, Vienna
[65] Communication Authority of Kenya, (2016).
[66] Ibid, (2016).
[67] ICT Authority, Kenya, "The Kenya Cyber Plan 2013-17, (2016)".
[68] Otuki, N.2014." Beijing Says Runda Fraud Ring Likely Targeted China." Business Daily, December 5. Available www.businessdailyafrica.com/Beiking-says-Runda-fraud-ring-targeted-China/-/539546/2546306/-/item/0/-/v9hr5bz/-/index.index.html. Accessed on 30 May 2018

fail to transversely protect the country from cybercriminals.[69] However, despite the multifaceted approach put in place in combating the threat in other developing countries, little information is available on Kenya's preparedness to face the nascent nemesis.[70] The war on cybercrime can only be won by having regional cooperation approach to cyber security that is strongly supported by member states. The need to create a Computer Emergency Response Team (CERT) is critical.[71]

The quest by Kenya to strengthen cyber security strategy is faced with a challenge of recognition and the need to seek partnerships with developed actors that can respond to emerging issues, (Kigen et.al.2014,41).[72] While the country has made impressive efforts towards this, there remains more action to address the growing cyber-security threats in Africa as a whole.[73] There is a need for a more practical approach to strengthen the existing processes as well as build capacity to deal with emerging issues.[74] This reality remains constant today and it is for these reasons that this study aims to analyze how cyber technology affect security in Africa, using a case study of Kenya.

1.9.1 Research Gaps

The relationship between cyber technology and in-security is a complex phenomenon but equally important. The development in the cyber space technology and the rising cybercrime present a relationship that is of concern to national security.[75] The existing literature shows that as technology advance, so does the threat scenery. According to case studies in developed countries of the West, academic articles about internet in Africa only discuss the impact of ICT on economic development,

[69] Ibid.p3
[70] Heeks, R. Stragegies for indigenizing IT production in developing countries. Paper presented at the IFIP and Kenya computer Institute conference on the Social Implication of Computer in Developing Counties, 23-25 March, Nairobi, Kenya.
[71] The East African, Kenya Launches Centre to fight cybercrime, (2016), p.89
[72] Kigen, P. C. Kitsutsa, C. Muchai, K. Kimani, M. Mwangi and B. Shiyayo. 2014 "Kenya Cyber Security Report 2014." Available www.serianu.com/KenyaCyberSecurityReport2014. Accessed 10 June, 2018
[73] Cassim, F. 2011. "Addressing the Growing Spectre of Cybercrime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players." Comparative and International Law and Justice South Africa 44:123-38.
[74] Ibid.p9
[75] Ley, C. 1984. 'Relations of Production and Technology.' In Technological Capability in the Third Words, edited by M. Fransman and K King. London: Macmillan Press.

education, health and other opportunities and challenges faced in breaching the digital technology gap.[76] There are few articles written about cyber security in the continent especially given the rising cybercrime which are mainly descriptive reports in nature or comments on specific events.

The cyber security situation in Africa is closely related to its development level of internet. Due to its weak economic base, the ICT has always lacked behind in terms of security awareness and appropriate legal system.[77] The lack of sound cyberspace security strategy implies that the continent is likely to present a breading space for criminals and terrorists.[78] Owing to the fact that Africa does not have technology of its own but relies on importation without a corresponding technology transfer, shows serious gaps in the continent. This is evident in the way the technology has been adopted which has resulted to poor enactment of laws and policies that has remained a challenge of in their applications.

It is therefore the expectations of this study to provoke national debate that will inspire generation of policies that will increase cyber security awareness at all levels. It is anticipated that the outcome of this study will help mobilize national and stakeholders' efforts to address the in-security caused by cyber technology.

1.10 Theoretical Framework

The study will employ Securitization Theory so as to comprehend cyber technology and in-security. The theory of securitization is similar to the opinions of scholarly work from Copenhagen School such as Barry Buzan and Ole Waever,[79] who argue on the central notion on state security is to survive.

[76] Gady, F. S. Africa Cyber wmd. Available at www. Foreignpolicy.com/articles/2010/03/Africa cyber.wmd. (2010), p.35.
[77] ITU.2015.ICT Statistics. Available www.itu.int.en/ITU-D/Statistics/Pages.stat.defult.aspx. Accessed on 30 September, 2017
[78] Sheldon B. John, "Deciphering Cyber power: strategy Purpose in Peace and War," Strategic Studies Quarterly, Summer, 2011. Available http//www.au.af.mil/au/ssq/2011/summer/Sheldon. Accessed on 20 August 18.
[79] Barry Buzan and O1 Waever 1991. People state and fear: an agenda for international security studies in the post-Cold war era, 2nd New York Reiner publisher. London.

Securitization can be presented as an issue when it is assumed to pose an existential danger to the existence of a referent object. In this regard the referent object is a state that is perceived to be under threat and require protection. According to Poeples & Vaughan-William, potent that when an issue qualifies to be considered as a security matter, it is politicized and if the threat is magnified, the matter becomes securitized.[80]

Consequently, securitization begins from a speech act from political leadership. This argument is further supported by Abrahamsen who argues that securitization is a socially constructed security threat which becomes represented and recognized as the state proceeds to use whatever means to respond.[81] Similarly, Buzan was quoted in Peoples & Vaughan-Williams adds weight by arguing that the threat and weaknesses have to be presented as existential threat to referent entity of securitization actors who endorse measures to be taken for instance cyber security. Owing to the increase in globalization and technology innovations has emerged as a threat in the cyber space domain which has had a substantial influence on state security.[82]

The increase and sophistication of cyber-attacks is arguably a prominent non-traditional issue in the national security agenda.[83] Sheptycki notes that the potential for cyber-attacks against a state critical infrastructure should therefore justify securitization of cyber technology and in-security, (Sheptycki, J, 2009).[84] Kenya has lately been a victim of international cybercrime with the most recent one in 2017 involving criminals from China, America and Europe.[85] This study notes that cyber-incidents in Kenya

[80] People & Vaughan-William 2010:77. Critical security studies: An introduction, London: Routledge.
[81] Abrahamsen 2005:57-58. Blair Africa: The political of securitization and fera, Alternative global local political 30:55-80.
[82] Kharouni, L. 2013. "Africa: A New Safe Harbon for Cybercriminals?' Trend Micro Incorporated Research Paper.
[83] World Economic forum (2015), "Partnering for Cyber Resilience. Towards the Quantification of Cyber Threats, in collaboration with Deloitte, 2015.P.9
[84] Sheptycki, J., Polishing, intelligence and the new human security paradigm: come lessons from the field intelligence theory:Key questions and debates, Studies in Intelligence, (London: Routledge, 2009) p.166
[85] Angence France Press. 2014 "Kenya Arrests 77 Chinese National in Cybercrime raids: The Guardian, December 5, 2014. Available www.tegurdian.com/world/2014. Accessed 02 May 2018.

have caused significant damage. As much as the potential for catastrophic cyber-attacks against critical infrastructures seems likely, hence cyber-security must be regarded as a national security issue.[86] The Government has increased the application of ICT in most of its business interactions which makes it a likely target for attack. Considering that the youths are the major users of the technology, they are likely to be penetrated because of lack of security awareness in the industry. This gap must be closed by deploying resources on research and development on cyber security. At present, there is a general feeling that knowledge and information on cyber security matters in Kenya and Africa are lacking. In this regard the securitization theory is most applicable in this study because the threat is existential and requires urgent action by the government, (Hansen & Nissenhaun, 2009).[87]

1.11 Research Methodology

The knowledge on cyber technology and in-security as an evolving security challenge in Africa will be done through qualitative research method which involves desk study of journal articles, academic papers and books on cyber security. The second method will involve analytical and descriptive research method which will explore cyber-attacks that are experienced in Africa and in particular Kenya. According to Leedy, the two methods will offer an insight on the status of cyber security in the continent.[88] This methodology therefore summaries the study design adopted which is appropriate and gives the researcher a good view of what they are really like in the area of study.

In evaluating the both the quantitative and qualitative information, this study will aim to demonstrate how cyber security defence is most needed in African today than has been before. The lack

[86] Nzwili, F. 2015. "China Kenya at odds over suspected Chinese Cybercriminals." The Christian Science Monitor. Available at www.csmonitor.com/World/Africa/2015. Accessed 08 September, 2018.
[87] Hansen, L. & Nissenhaum, H., 2009 Digital Disaster. Cyber Security and Copenhagen School International Studies Quarterly, Volume r, pp.1-25
[88] Paul. D. Leedy, Practical Research. New Jersey: Prentice – Hall, (1997), p. 1.

of strategies to mitigate the problem among Africa nations is disturbing, as it suggests failure of governments to tackle cyber security seriously.

1.11.1 Research Design

This study will be presented in chapters which according to Nachmias and Nachmias, the concept is to guides the researcher in the course of collecting, analysing and interpreting observations.[89] This research employed exploratory study as a research design which provides the researchers with a good view of what they are certainly like. This study utilized both quantitative and qualitative research approach across the steps of the research process in the study of cyber technology and in-security relationships in Africa. The quantitative data was examined using the Statistical Packages for the Social Science (SPSS) SP 500 while qualitative data was analyzed using content analysis. The methodologies used in this study provide a platform on which all the issues and elements to do strategies for addressing cyber threats.

1.11.2 Population Size

This study targeted a population size of 75 people drawn from the following organizations who include professionals and technical staff in IT. These organizations include Ministry of Foreign Affairs, Kenya ICT Authority, Communication Authority of Kenya, National Intelligence Services, the Ministry of Defence, National Police Service, Kenya Revenue Authority, ICT Business Organizations, Banking Sector, Safaricom and Universities as shown in **Table 1.1.** Due to time constraints, the researcher utilized stratified sample method targeting IT professionals who included executives, senior managers, junior managers and senior technical staff from the sample. This group was chosen because of the quality of information that was required.

[89] Chava, F. and Nachmias, D Research Methods in Social Sciences. London, (1985), p. 11.

Table 1.1: **Population distribution**

SERIAL	ORGANIZATIONS	TARGET POPULATION
1	Ministry of Foreign Affairs, Kenya	7
2	Ministry of Devolution	3
3	Communication Authority of Kenya	4
4	Kenya Revenue Authority	4
5	Banks (KCB & Coop Bank Nairobi)	5
6	Diplomats (Botswana And Somalia)	4
7	Advocated (Asa & Asa Adv)	7
8	Universities – UoN, USIU & Tech Univ of Nairobi	3
9	Kenya Defence Forces Headquarters	5
10	National Police Service Headquarters	3
11	National Intelligence Service Headquarters	3
12	Safaricom	4
13	ICT Business Organizations (Interfina House Nairobi)	8
14	Others (Cyber Café Nairobi)	15
TOTAL		**75**

Source: Author (2018)

Denzin and Lincoln, agree that this type of judgemental sample can only be applied when the researcher is certain on which type of people or units are typical of the population in question.[90] In this regard the population chosen to participate in the study was drawn from the institution head offices in Nairobi. The

[90] Norman, K., Denzin, Y and Yvonna,L. The Dage Handbook of Qualitative Research, (2000), pp. 105-117

sample chosen was a representative of the population sample that could be studied to represent the entire unit of the population.[91]

1.11.3 Sample Size

The sample was guided by Taylor's guidelines that a sample should neither be too large nor small as the earlier wastes resources unnecessarily and the later limits the generalisation of study findings. This researcher settled for a sample of representativeness of 66.7 percent as indicated in **Table 1.2.**

Table 1.2 Sample Size

SER	ORGANIZATIONS	POPULATION	SAMPLE SIZE	PERCENTAGE
1	Ministry of Foreign Affairs, Kenya	7	5	
2	Ministry of Devolution	3	2	
3	Communication Authority of Kenya	4	-	
4	Kenya Revenue Authority	4	1	
5	Banks (KCB & Coop Bank Nairobi)	5	5	
6	Diplomats (Botswana And Somalia)	4	4	
7	Advocated (Asa & Asa Adv)	7	2	
8	Universities – UoN, USIU & Tech Univ of Nairobi	3	3	
9	Kenya Defence Forces Headquarters	5	5	
10	National Police Service Headquarters	3	3	
11	National Intelligence Service Headquarters	3	3	
12	Safaricom	4	-	
13	ICT Business Organizations (Interfina House Nairobi)	8	7	
14	Others (Cyber Café Nairobi)	15	10	
TOTAL		**75**	**50**	**67%**

Source: Author (2018)

[91] Ibid, (2000), p. 121.

1.11.4 Sampling Methods

The researcher made use of stratified random sampling to select the respondents for the study.[92] This was done dividing the targeted respondents into their respective units, functional areas, departments and later random sampling used to select the actual participants for the study based on the proportional size of the subgroups. This method was applied ensured that all the different units of the population were duly represented in the study. 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.

1.11.5 Data Collection

The research was based on quantitative research methods. The one on one interview was used so as to obtain facts and minimize prejudices. Purposive sampling was also used to produce maximum variation within a sample, the respondents were chosen based on their work in cyber security studies. The information was obtained through questionnaire to assist in the interview with the ICT professionals and technical staff. The interviews provided valuable information for the study.

A pilot collection and analysis of the interview guide was conducted to gauge the outcome and correspondence to the purpose of the study. Further, the study took steps to make sure that the research was done to the required standards according to the University guidelines. The analysis of the data incorporated the coding of the study content into similar themes based on focus groups interviewed and later analyzed using content analysis and inferential statistics. The content analysis of the research is a method used to make valuable inferences by coding and interpreting and textual materials to make meaning to the study.

[92] Holloway, P. and Galvin,L. (2016), p. 9.

1.11.6 Procedure of Data Analysis

The data was collected through guided questionnaire interviews, libraries and internet was analysed using descriptive statistics and inferential calculations and presented in form of narrative, charts, graphs and tables. This study used interpretive content analysis and inferential statistics in analysing the research findings. Denzin and Lincoln, potent that the analysis involves a methodical classification of relevant material from the sample thus permitting application of detailed analysis in this study. The method of aanalyzing the documents involved coding of the content into themes according to similar focus groups and later analyzing the transcripts. A rubric (the cyber technology and insecurity variables under study) was used to grade or score a document. From the interpretation, the researchers were able to draw interpretations about the problem and made recommendations accordingly.

1.11.7 Summary of the Chapter

This chapter began by a brief background to this study, statement of the problem, research hypothesis, its significance and research objectives were outlined. The subsequent chapters explore the cyber technology security nexus in Africa. It gives an elaborate background of cyber technology as a source of development and threats to security in Africa. This study therefore first delves into the theoretical concepts underpinning cyber technology and its relationship with insecurity. The literature review is arranged in such a logical way which enhances an understanding to all the research questions outlined.

The method chosen enables this researcher the opportunity to focus more into cyber technology development in order to gain understanding on how it affects national security. The secondary data was mainly used to generate understanding and identify gaps to the study. After collecting field data, the researcher used tables to assist in the analysis interpretation and finally make recommendations related to the findings.

CHAPTER TWO

THE CYBER TECHNOLOGY- 'IN'SECURITY NEXUS IN AFRICA

2.0 Introduction

This Chapter explores the cyber technology – 'in'-security nexus in Africa. It gives an elaborate background of cyber technology as a source of development and threats to security in Africa. The internet technology has fundamentally transformed the continent's political, economic and social-cultural lives. The internet penetration in Africa has not been without the challenge of insecurity resulting from its use; which is of concern to the continent. The chapter also presents analysis of the findings from the field in relations to the objective under study.

2.1 Africa Cyber Technology Situation

There is a general agreement in the present day that technology contributes the growth of economic and social development of nations.[93] This has called on African countries to develop national technology strategies in line with their national development agendas. In order for Africa to benefit from this technology, it requires to develop a culture of IT which will be applied in all sectors of government, industry and service sectors.

Successful IT use engenders adoption and development of the technology that is suitable to address existing needs of economic and manpower capabilities in African states.[94] IT refers to technologies that are based on computers and telecommunication, including computer systems that offer

[93] Hansson, S. O. (2015). The role of Technology in Science: Philosophical perspectives. Royal Institute of Technology. Stockholm, Sweden

[94] Woherem, E.E. 1991b. Information technology and Africa: An appraisal of the present situation and future potential. Project Appraisal, Vol.6, no. 1, March 1991.

a means of storing, retrieving and communicating vast amounts of data and information quickly and cheaply.

However, Africa lacks the knowledge and expertise with which to design and develop new technologies that it can use to enhance its industrialization. It is imperative for Africa to establish a functional system of planning to enhance its technology and economic development. Africa is faced with the problem of how to gather, store, communicate and analyze data resulting from skill shortage. These means that most organizations both public and private use inadequate personnel to plan run its institutions. Instead it depends on imported experts for its expertise and to operate, maintain and implement machines. Import of already build Expert System (ES) such as Computer Aided Design (CAD) and Computer Aided Instructions (CAI) systems can help in the transfer of technology.[95]

While, the internet history in Africa is short, the new cyber technology is spreading fast in the continent, (Symantec, Corporation report (2013).[96] The technology has changed the business landscape with the continent witnessing increased usage of internet penetration in the last decade. Along with this, cybercrime is steadily growing while the relevant legal framework and law enforcement capacity is lagging coupled with weak public cyber security awareness.[97] Fortunately, most countries in the continent have awakened to the reality of cyber-attacks and have stated to appreciate the need to fast track institutional framework in cyber security governance, (Evans 2011).[98] This threat has meant the continent to rethink how it can better leverage the benefits derived from cyber technology use by

[95] Gane. C. 1990. Computer – aided Software Engineering: The methodologies, the Products, and the future. Englewood Cliffs, New Jersey: Prentice Hall
[96] Symante Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18. Available from www.symantec.com/content/en/us/enterprise/other_resources/b-ustr_main_report_v18_2012_21291018.en-us.pdf. Accessed on January 2018.
[97] Kenya Cyber Security Report, (2016), p. 14.
[98] Evans, D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything'. Cisco white paper Cisco Internet Business Solutions Group, (2011), p. 118.

developing institutional design for cyber security governance.[99] Learning from her developed partners in the west and Non-Governmental Government (NGO) advocacy, Africa is likely to be included in the global cyber security forums. However, the Western cyber security design framework still remains a challenge in practice in the African culture and traditions.[100]

The cyber security situation in Africa is strictly related to individual country's level of internet growth. Due to weak economic base, the development of information and communication industry has been observed to be lagging as compared to other developed nations of the world. Since the laying of the submarine cables, Africa has been linked to other continents of the world. This development has increased the continent broadband network coverage significant and the number of internet users has equally grown. According to ITU report of 2014, the growing ICT entrance in Africa has enlarged the Internet bid as compared to countries of Asia and Latin America (ITU, 2014).[101] The continent registered over 300 million internet users which was estimated at 27.5% of the total population, (Moeng, 2011).[102]

According to a report by Communication Authority of Kenya (CAK) of 2017, on the internet usage, there are an estimated 27.8 million internet users in the country. As internet usage continues to grow, the number of internet security incidents continues to rise.[103] The increased dependence on

[99] Asia Pacific Computer Emergency Response Team. The Cyber Green Initiative: Improving health through measurement and mitigation', concept Paper (Japan: Japan Computer Emergency Response Team Coordination Centre, 2012), p. 34.
[100] Holt, T.J. Sub-cultural revolution. Examining the influence of on and off-line experiences on deviant subculture. Deviant behavior, 28. (2007), p. 171 – 198.
[101]ITU (2014) 'World Telecommunication/ICT Indicators database', 18th edition. Available at www.itu.int/en/ITUD/Statistics/Pages publication/wtid.aspx[Accessed:7 January 2018]
[102] Moeng, B. Reasons to invest in Africa ICT. IT News Africa, (2017),p. 14.
[103]Gordon Crvitz, (2012), "National Security Challenges of the 21st cent Africa is a continent with enormous natural resources and economic diversity, but remains underdeveloped.[103] In the past decades, Africa has experienced high and growing economic development that has driven experts to argue that the Africa is at a turning point with respect to its developmental agenda ready to become a key participant in the international economy, particularly in the 21st century.[103] For most African countries, the annual rate of economic growth increased by 1.8%. This led to enhancements in numerous areas such as trade and government resource mobilization", Cyber Security Wall Street Journal, February, 2012: Available http//www.Online article/SB142 4052 90 203918304577 243423337326 122. Accessed on 20 June, 2018.

information technology has exposed Kenya's prime institutions to calculated security threats with adverse consequences, (Rahemtulla et al, 2012).[104] It is evident that Kenya's' institutions are ill prepared to respond to cyber security threats due to lack of capacity in training and institutional framework. Though there are different initiatives in place, the need to seek wider cooperation with other players internationally is most welcome.[105]

2.2 Africa Cyber Security Concept

The Africa cyber security concept emerged in 1990s after the cold war period when computer technology came to light. Initially, the term was thought to be related to networked computer, but later it was confirmed to be emerging from new cyber technologies.[106] Owing to the increasing threats, the Africa Union (AU), in 2014 embraced the Convention on Cyberspace Security and Protection in Malabo, Guinea.[107] Although the Convention focused on Cyber Security; the concept was not well understood except the explanation in the convention text. This is because cyberspace lies in the expansive global field. The Convention envisaged regulating the evolving technological domain which set forth the cyber rules on security as a critical step in establishing credible digital space for protecting the infrastructure.[108]

Arising from the convention, African states adopted different strategies to contain the threats peculiar to their environment.[109] Most nations such as Kenya, Uganda, Cameroon and Botswana started

[104] Opendata.go.ke. Open Data Network. Available http//www.opendataresearch and majee (2012) and Rehemtulla, et al (2011). Accessed 05 February, 2018.

[105] Ranz-Stefan, G Foreign policy: Africa's internet threat, National Public Radio, (2010), p.29.
[106] Singer, P. & Friedman, A., 2014 Cyber security and Cyber war. What everyone needs to know. New York: Oxford University Press.
[107] African Union, "African union Convention on Cyber Security and Personal Data Protection," p 1-3
[108] Ibid p5
[109] Schell, B. Ho. & Clemens, M. "Cybercrime: A Reference Handbook," ABCCLIO, (2004)

to enact cyber legislations and establish sub-regional collaboration instruments to combat cybercrime.[110] On the other hand, West African Economic Community nations (ECOWAS) chose to adopt the "Commonwealth Model Law on Computer Related Crime and the European Council under Budapest Convention on Cybercrime and Directive to Fight Cybercrime".[111]

Through the support of International Telecommunications Unit (ITU), the Kenya Government in 2012 established the "Kenya National Computer Incident Response Team Coordination Centre (KE-CIRT/CC)". This unit was to assist in providing advice on technical supervision of cyber related crimes. The KE-CIRT/CC was delegated to guide and advice the Government on issues concerning national cyber security and coordinating all other agencies both local and international on cyber incidence response mechanism. However, since its inception, the organization has remained dormant hence casting doubt on its role as a key national agent. This has also created doubt in its competence and therefore has lost its relevance, Kigen et al.2014, 48).[112]

2.3 Cyber Security Landscape

The cyber security threats in Africa are similar in characteristics to those taking place globally. However, the internet infrastructure connections in Africa distinguish it from the rest of the world.[113] The reason for the irregular connectivity is due to lack of technological capacity which makes it susceptible to attacks. This is true especially the banking and public sector systems networks relies on machine run software which is obsolete and hence no longer supported by the manufacturer.[114]

[110] Juma V. (2010) online Shopping Kenya Consumers out of KRA Reach. http//www.businessdailyafrica.com. Accessed 08 December 2017.
[111] "Nigeria's president Jonathan signs the Cybercrime Bill Intl Law", May16, 2015. Available http://techloy.com/2015. Accessed 21 February 2017
[112] Kigen et al.2014,48
[113] Gercke, M. The Slow Wake of a global Approach Against Cybercrime, Computer law Review International, (2006), p. 89.
[114] Cybercrime id defined as a broad range of illegal activities committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

The mobile industry also raises similar concerns of selling out of date software. Alongside this, there is a lot of unsupported software and upgraded servers which exposes the whole ICT infrastructure to attacks. Another challenge is lack of reporting of cyber security incidents by some organizations regarding cyber-attacks.[115] This situation denotes the difficulty to establish the extent of cyber-attacks in Africa which makes it hard to find solutions. Lack of capacity in information sharing, effective legislation and enforcement are key weaknesses in Africa internet infrastructure security, Norton Cyber-Crime Report 2016.[116]

2.4 Cyber technology In-security Nexus

The future of Africa science and technology is promising, despite the unprecedented advances of insecurity that are also growing fast.[117] The underground criminals are equally very innovative and are fast to adapt to any emerging technologies.[118] Most of them have now developed their own encrypted communication networks, for example the Mexico Narcotic criminals and Al-Shabab with Improvised Explosives Devises (IED) in Somalia.[119]

Cyber technology has made the world increasingly open despite the huge benefits for society. While this is the situation, the criminals have also invested and deploy the same technologies in their field operations.[120] For example, the Al-Shabab terrorists in Somalia have resorted to the use of remotely controlled IEDs as weapon of choice against African Mission in Somalia (AMISOM) troops. The IEDs

[115] Goel, S. (August 2011) "Cyber warfare: Connecting the Dots in Cyber Intelligence" Communications of the ACM; Vol.54, No.8, 132 – 140.
[116] Norton Cyber-Crime Report, (2016), p. 79.
[117] Ben Bernanke. Promoting Research and Development: The Government's Role. Journal on Science and Technology. Vol 27, No 4 Nov 2011.
[118] "Global Cyber security Agenda "Brochure" Corporate Strategy Division, International Telecommunications union, 2007: URL: Available (http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf), last accessed: 12 June 2018
[119] Johnson, Neil F., Juan Camilo Bohorques, Zhenyuan Zhao, and Mike Spagat (2007). Common Complexity Underlying Insurgent Wars and Terrorism: A Contribution to the Workshop on Disrupting IED Terror Campaigns.
[120] Greers K. (January 2009) "the Cyber Treat to National Critical Infrastructures; Beyond Theory" Information Security Journal: A Global perspective;18 (1):1-7

are homemade bomb technology which have been evolved over time and now come in many forms and levels of sophistications.[121] The IED innovations are initiated using cell phones that are remotely operated from a distance to avoid detection. Given the advancement in technology, the criminals have clearly shown their ability to seize the opportunity for their own advantage.[122]

2.5 Africa Cyber Security Resilience

Africa cybercrime and security discussions have tended to highlight hacking of information, terrorism, or use of infectious malware amongst others.[123] It is evident that very little attention has been given to issues where the continent is able to withstand because of lack of knowledge and capacity to foresee threats from cyberspace.[124] The continent's cyber security resilience is intended to ensure that in the occasion of a cyber-attack there are measures to mitigate in the event of failures, the system does not completely collapse.[125]

Cyber resilience concept calls for a broad based approach when dealing with cyber security, in order to develop strategies and measures which have been elusive to handle before, (Cassim 2011).[126] As observed the Western powers approach on the matter has been informed by their interest in Africa especially on issues dealing with fighting terrorism. This effort has been at the expense of in-depth cyber

[121] Bale, Jeffrey M. (2007). Some Pareliminary Observation on Jihadist Operation in Europe. In Workshop on Determining a Research Agenda for Disrupting IED Terror Campaigns: finding the Weak Links. Irvine,CA.
[122] Brigadier General Barbara Fast, C2, CJTF7, for Defense Intelligence Agency, through Commander JCMEC, memorandum, Iraqi Theater of Operations (ITO) Combined Explosives Exploitation Cell, October 23, 2003.
[123]Farwell, J. P. & Rohozinski, R. (January 2011) "Stuxnet and the future of Cyber War" Global Plitics and Strategy, Vol.53, No. 1, 23-40
[124] Lewis, A. J. Assessing the risks of Cyber Terrorism, Cyber War and Cyber Threats, Journal of Centre for Strategic and International Studies, Washington DC, (2002), pp.22-27
[125] Ganuza, N., Hernandez, A. and Benavente, D. (June 2011) " An Introductory Study to Cyber Security in NEC" NATO Cooperative Cyber Defense Center of Excellence – Tallinn, Estonia
[126] Cassim, F. 2011. "Addressing the Growing Specter of Crime in Africa. Evaluating Measures Adopted by South Africa and other Regional Players". Journal of East Africa Studies 7(2).

security programs for the entire continent, (Ploch 2010).[127]

It is on the basis of this the "AU Convention on Cyber Security and Personal Data Protection", a body that handles continental cyber preparedness issues, has raised concerns on cyber security situation in the continent with different security awareness levels.[128] According to routine activity theory, cyber threats thrive when there is availability of suitable opportunities and the absence of adequate protection measures.[129] In translating this argument to cyber resilience measures in Africa, shows that the efforts are not without challenges. The pursuit for well synchronized cyber security methods to address increasing cyber-attacks need to be treated with more political understanding than it is today.[130]

2.6 Africa Cyber Security Framework

Africa development into the internet technology of doing business lacks institutional framework to address the threats internet poses. Whereas, a few institutions have been established to fight cybercrimes, they are still weak to deal with the challenges presented by technology. The continent lacks clear policies on cyber security and the available laws cannot lead to any meaningful action.[131] The case of cybercrime in Kenya is a pointer to the weaknesses which are recognized to being as a consequence of absence of a government intervention to track and monitor online activities of suspects.[132] This argument is true considering the way in which enforcement on perpetrators has been handled previously.

[127] Ploch, L. 2010. "Countering Terrorism in East Africa: The US Response." CRS Report for Congress, Congressional Research Service.
[128] Macharia, J.2014. "Africa needs a cyber security Law but AU's proposal is Flawed, advocated say." Available www. techpresident.com/news/wegov/24712/africa-union-cybersecurity-law-flawed. Accessed on 30 June, 2018
[129] Cohen, L and Felson, M. Social change and crime rate trends: A routine activity approach, Americac Socialogical Review, (1997), pp. 588-589.
[130] Ibid pp. 594.
[131] Akogwu, S. *An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University*, Zaria (Unpublished B.Sc project). Department of Sociology, Ahmadu Bello University, Zaria, (2012), p.75.
[132] Mengo, B. Urban Cyber Space under Criminal Siege, (2011), p.67.

The Kenya cyber security laws are week and rarely provide effective remedies to suspects. Equally, in South African legislation, the victims are free to report cybercrimes owing to lack of enforcement. [133]

This is a gap that is exacerbated by the weak political and institutions to enforce the law, and corrupt which reflect the lack of goodwill to fight the crime.[134] For example, it is noted that some high-ranking officials in the government in Nigeria were involved in cybercrime either to hacking bank accounts or steal government information.[135] In many instances, the cybercrime laws have been noted to have gaps that allow hackers to operate without detection. The Kenya Communication (Amendment) Act 2009 prohibits hacking of an imposter website.[136] Equally, the court system and law enforcement agencies lack adequate computer knowledge competence to be able to effectively combat cybercrimes (Daily Trust, 2010).[137]

However, it is encouraging to note that with the enormous losses incurred through cybercrimes, Africa is waking up in cyber security initiatives. There is now putting cyber security awareness measures through social learning programmes for academic writings.[138] Similarly, a framework is being developed to deal with cyber threats in the continent. Among these efforts is the establishment of cyber security export groups that are responsible for handling computer security events at both international and national levels. In Tunisia, for example has established a first African Cyber National Security Institute known as the "Tunisian Computer Emergency Response Team Coordination Centre (CERT

[133] Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi and B. Shiyayo. 2014. "*Kenya Cyber-Security Report 2014*." www.serianu.com. Accessed on 13 December, 2017.
[134] Balancingact-africa.com, (2010). Impact of Cyber Fraud on Kenyan Banking Sector, Devastating, p.23.
[135] Kornakov, K.(2006). Police forces in East Africa Will have a New Hi-tech lab at www.viruslist.197753850. Accessed on 08 December, 2017
[136] ICT Authoriry, Kenya, the Kenya Cyber Plan 2013-2017, (2016).
[137] Otieno, J. 2014. "Worries over New Avenues of Cybercrime." The East African, September 22 at www.theestafrican.co.ke. Accessed on 20 January, 2018.
[138] Baumartner, F. R. and Jones, B.D. (1993), Agenda and Instability in America Politics. Chicago: University of Chicago Press.

TCC)" which receives support from ITU (ITU, 2009).[139] Others which have followed same route are Morocco, South Africa, Kenya, and Cote d'Ivoire which have established Africa Coordinating Centre Africa CERTs in 2011, (Wanjiku, 2011).[140]

Similarly, some African countries are also improving their efforts to fight crime. Further, Tunisia and South Africa have gone ahead to develop national cyber security framework and legislation for identification of electronic devices. These countries have strengthened their law enforcement skills and capacity to deal with cyber threats. Further, Nigeria has equally followed and established a user awareness programme as a strategy for national cyber security edge (Gady, 2010).[141] The East Africa Community (EAC) states have also followed the example and are on discussions to establish a cyber-science centre of excellence, (Muwanga, 2011).[142] Likewise, Kenya had planned to establish a cybercrime laboratory referred to as forensic lab for use by national police, but this was not actualized due to corruption (Kornakov, 2005).[143]

2.7 CHAPTER DATA PRESENTATION, INTERPRETATION AND ANALYSIS

To better understand the correlation of cyber technology-security nexus, analysis was conducted using ten variables between cyber technology and in-security. The analysis, Fig 2.1 revealed that there are strong correlations between technology and in-security as technology increases so is the threat level. However, the threat is only normalized when appropriate measures and strategies are taken to mitigate the effect as shown in Graph Fig. 2.1. In the circumstance, this analysis validates the hypothesis that

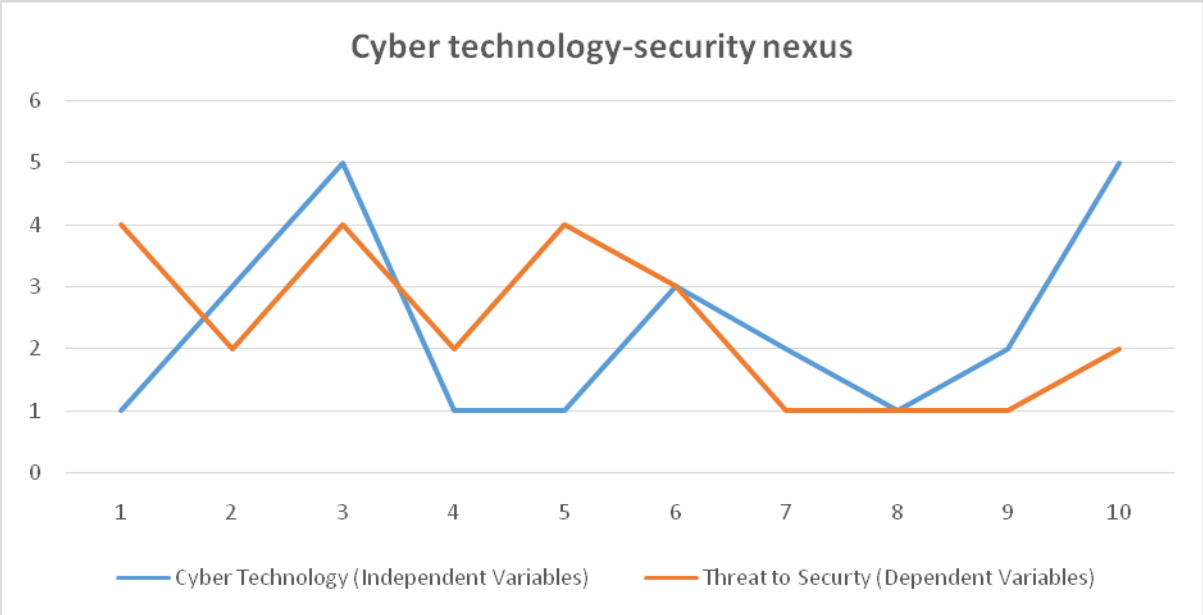
[139] Draft Meeting Report: ITU Regional Cyber Security Forum for Africa and Arab States held in Tunisia, Tunisia (4-5) June 2009.
[140] Wanjiku, R. (2011), Rising Cybercrime Pushes African Government to Take Action. Computer world Kenya. Available www.news.6EF9B560-ODDE-E2CB-4D0981F70155CC24. Accessed on 05 December, 2017.
[141] Gady, F.S. Nigeria National Cyber Security Initiative (2010, p. 104.
[142] Muwanga, D. (2011), east Africa Asked to Build Cyber Science School. Available at www.busiweek.com/11/opportunities/1997//east Africa science school. Accessed 6 December, 2017.
[143] Kornakov, K. (2006), Police Forces in East Africa will have a new Hi-tech lab. Available at www.viruslist.com.197753850. Accessed 03 December, 2017.

cyber security is influenced by the advancing technology. This relationship proves the validity of the research which agrees with Mugenda & Mugenda, 2003) on what the researcher is interested with when dealing with both dependent and independent variables. This corroborates with the literature in Chapter 2 para 2.1 on Africa technology situation and this has influenced development.

Table 2.1: Cyber Technology-Security Nexus

Respondents	**Cyber Technology (Independent variables)**	**Threat to Security (Dependent variables)**
1	1	4
2	3	2
3	5	4
4	1	2
5	1	4
6	3	3
7	2	1
8	1	1
9	2	1
10	5	2

Figure 2.1: Cyber Technology-Security Nexus



Source: Author (2018)

2.8 Summary of the Chapter

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 shown in Fig 2.1 above. Though the level of IT penetration in Africa is relatively high, the reliance on technology in business and daily life has equally grown insignificantly. Nonetheless, the trend of cyber technology development is positive and there are several efforts being applied to withstand the challenges on security.

The lack of appropriate cyber space use in Africa coupled with the failure of institutions dealing with cyber security to keep pace with the advancing digital technologies has undermined the efforts of growth. This is evident from the fact that the legal framework and enforcement are not synchronized to move in tandem to the cyber landscape. The result of inconsistencies is increase of risks in cyberspace which will threaten the national security due to the growth of technology. While it is true that cyber

technology has presented some threats to users, the positive aspects of the technology in socioeconomic development is evident in countries of the West, may also be possible in Africa.

CHAPTER THREE

THE EMERGING PATTERNS OF CYBER TECHNOLOGY AND NATIONAL SECURITY DILEMMA IN KENYA

3.0 Introduction

This chapter explores the emerging patterns of cyber technology and national security dilemma in Kenya. It provided a background of cyber technology situation in 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 knowledge of the users. This study proceeded to collect data from the field that will be used to analyze the research question and objective under study. The study presents this results in the chapter analysis

3.1 Kenya Cyber Technology Situation

Cyber technology in Kenya has become important to daily life of persons, governments and businesses enterprises. Many African nations are still emerging to embrace information technology and several companies in telecommunication seeking economic opportunities are proposing more solutions.[144] Yet, with the exponential increase in use emerges the problem of data for malicious purposes. This is a phenomenon that is rising in number, complexity and effect, (Romero-Mariona et. al, 2009).[145]

With the emerging internet of things technologies, has complicated the network and threat leading to a security dilemma. In a few couple of past years, utilization of internet in Kenya has

[144] Gergle, M. understanding cybercrime a guide for developing counties; Geneva international telecommunication Union, (2011), p.89

[145] Romero-Mariona, J., Ziv, H., Rchardson, D. J., & Bystritsky, D. Towards usable cyber security requirements. In proceedings of the 5th Annual Workshop on Cyber Security and information intelligence Research; Cyber Security and Information Intelligence Challenges and Strategies, (2009), p. 64.

increased due to demand in mobile usage. According to Communication Authority of Kenya (CAK) report 2016, there were 27.3 million internet subscribers in the country. As this number grow, the same applies to internet security incidences reported. This situation results to cyber security dilemma. The increase on cyber technology use has exposed the country's institutions to premeditated security threats with likely severe consequences. These institutions have been known to be prime targets for insider attacks as well as cybercriminals.[146]

While cyber technology and security global trends present an increase in complexity, the trends locally are fairly manageable though upsetting. Most of issues highlighted in this thesis are not new however, they point at vulnerabilities and a lack of national strategies to address the problem. The reasons for this weak spot is that the country's local institutions are poorly resourced to respond to cyber security threats. Whereas, there exists varied initiatives intended to address the threat issues, they are not appropriate enough to fully deal with the current security challenges.

As Kenya prides of penetration rate, most of the internet networked computers are infected with malicious programmes that make the entire infrastructure susceptibility to online fraud. The existence of botnet activity in Kenya poses a threat to the country's critical cyber technology. A botnet is described as a network of infected computers controlled by cybercriminals without permission of user. The botnet threats have greatly increased with the development of cyber technology environment and its complex nature. This threat has been known to have serious consequences to most societies, especially when it is used to coordinate attacks directed at key national infrastructures.[147] This type of crime mainly resulting from botnets exposes the users to risks of loss of personal data. Owing to these threats some

[146] Regarding the possibilities and technology available to access the Internet in developing countries, see: Esteve/Mechin, Devices to access Internet in Developing countries, available at www2007.org/workshop/paper_106.pdf. Accessed 30 May 2017

[147] Serianu Consultants in Cyber Security (2015); available at www.usiu.ac.ke/oncampus/news/296-serianu-usiu-africa-pkf-consulting –Launch-Kenya-cybersecurity-report-2015.

organizations have ceased processing business online for fear of attack and instead have opted for secure modes such as intranets which utilize Local Area Networks (LAN).[148] Consequently, cyber threats which target desktop computers have switched to the use of mobile ecosystem such as mobile phone devises.[149]

According to ITU report (2014), mobile threats are on increase because of the increased use of smart phones which have been associated with cyber insecurity.[150] For example, in 2011 nearly 64 percent of mobile threats were targeted on mobile smart phones such as Androids and BlackBerry. In 2012, these threats reached 94 % and were attributed to the increased use of mobile malware advances which seem to defy intrusion prevention devises such as firewalls.[151] In the circumstance, Kenya faces high risk of attack due to proliferated use of Android phones which the Communications Authority of Kenya (CAK) is working on to remove possible counterfeit mobile devices.[152] Due to globalization and over dependence on ICT, Kenyans are increasingly exposed to cyber-attacks due to lack of suitable protections.[153]

[148] Clark, K., Stikvoort, D.,Stofbergen, E., & Van den Heuvel, E. (2014) A Dutch Approach to Cybersecurity through Participation. Security & Privacy, IEEE, 12(5), 27-34.
[149] ENISA,"ENISA treat Landscape 2013 – overview of Current and Emerging Cyber Threats," 2013, available at www.enisa.europa.europa.eu/activities/risk-management/evolvingthreat-environment/enisa-threat-lanscape/enia-threat-landscape-2013-overview-of-currentand-emerging -cyber-threats/at download/full Report.
[150] Ibid
[151] ITU,"Understanding Cybercrime. A guide for developing countries"; Symantec, "Internet Security Threat Report;"2014, available at www.symantec.com/content/en/us enterprise/other_resources/b-istr_main_report_v19_21291018.en-uspdf;Kaspersky. Accessed 11 June, 2017.
[152] Macharia Kamau, "Kenya Wants EAC States to Hasten Fake Phone Switch Off," Standard Digital, 28 June 2013.ABLE www.standardmedia.co.ke/business/article/2000086969/kenyawants-eac-states-to-hasten-fake-phone-switch-off 7/07/2013; Winfred Kigwe, "Kenya: 1.9 million Fake Phones Shut," All Africa, 2 October 2012, available at www.allafrica.com/ stories/201210020512.html. Accessed on 06 February, 2018.
[153] Daily nation August 3,2016

3.2 Kenya Concept of Cyber Crime

The concept of cybercrime is understood as unlawful action that utilize computer networks as a target tool for criminal action that include all aspects of electronic cracking to denial of services.[154] Cybercrime also includes crimes in which they use ICT platforms to enable illicit activity. Cyber security according to Kenya Information and Communications Act (2013) is defined as the "the collection of tools, policies, security concepts, security safeguards, guidelines and best practices that can be used to protect the cyber environment".[155] Cybercrime target Government offices, Banking institutions, financial services and mobile money, industry and Telecommunications sector.[156] The cost of cybercrime is colossal and can be accessed directly and indirectly taking into account various issues such as loss of financial assets and sensitive business information, and reputational damage to the organization. In 2015, Kenya lost Kshs. 15billion to cybercrime, with 4billion of it taking place within the banking sector (Serianu).[157]

3.3 Kenya ICT Environment

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.[158] 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. One of the core priority areas for the government is to utilize e-economy capability to create employment and wealth as part of

[154] Chavan, G. R., Rathod, M. L., &Naik, N. (2010). Cyber Crime: A Study. SRELS Journal of Information Management, 47(4), 465-472.
[155] Kenya Gazette Supplement, ACTS, (2013), p. 19.
[156] Kenya Cyber Security Report, (2016), p 4.
[157] Kenya Cybersecurity report, (2015), p. 9.
[158] Wechuli A. On Cyber Security Assessment Framework: Case of Government Ministries in Kenya; International Journal of Technology in Computer Science and Engineering, 92004), p.3.

national development strategy in achieving Vision 2030 ICT flagship on security of the individuals and of property.[159] This goal has been realized through adoption of appropriate technologies of mobile banking, internet and broadband communications which connects the country to the global village. However, this technology presents new challenges that result in extensive damage to economic growth, national security and critical infrastructures.

Kenya, ICT has remained a vital component of the national growth of the economy. The sector is not a standalone component of the national economy but accounted under Transport and Communication sector. Consequently, it becomes difficult to follow through the impact of ICT to the economic growth as an individual sector as opposed to other countries whose ICT is considered as an autonomous sector, (Kenya ICT, 2014).[160] The International Standard Industrial Classification (ISIC), is the commonly used classification to define ICT as economic an autonomous sector. The Kenya National Bureau of Statistics (KNBS) is now considering adopting this classification in collaboration with Communications Authority of Kenya (CAK).[161]

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. Several cases related cybercrimes with criminals attempting to break into banks and Automatic Teller Machines (ATM) have been reported in Kenya.[162]

[159] Kenya Vision 2030 of October, (2007), p. 8.
[160] ICT Authority, "Kenya's ICT Master Plan 2014-2017;" ICT Authority and C4DLab, "Cybersecurity Training," 2014.
[161] Kenya Cybersecurity report, (2015), p. 9.
[162]Central Bank of Kenya, December 2008 Survey on Bank Charges and Lending Rates. Available www.centralbank.go.ke/deownloads/bsd/Survey2009.pdf. Accessed 22 April, 2018

3.4 Cyber Technology Trends and Security Threats

Kenya is one of the members of East African Community (EAC) whose economy is fast growing to keep pace with the new demands of digital technology (David, 2007).[163] With over 25 million out of a population of 50 million internet users in Kenya, the country is ranked position four in Africa which translates to equal number of cybercrime cases, as compared to Nigeria, South Africa and Egypt which are leading, (Misiko 2014).[164] Cyber-attacks are increasingly evolving faster than the defence measures to respond to such threats.[165] Between the year 1980 to 2016, Kenya experienced a number of sophisticated technology and social engineering attacks from hacktivists targeting financial institutions. The current cyber security threat trends tend to target both public and private organization. These threats are categorized into three groups as follows; Malware, Social Media attacks and Frauds.[166]

3.5 Emerging Cyber Threat Environment

The Kenya cyber-attacks have been observed to take place in an environment which fevours attackers. Since the cyber infrastructure is open by design, and owing to its interconnectivity against security requirements, the attacker has an advantage over defender.[167] This situation implies that there are few obstacles to criminals' entry in the cyberspace on the physical world coupled with weak government choice in the use of force. This situation gives the enemy with limited resources to exploit the weaknesses without interruptions. The introduction of new technologies has completely lacked in security elements. This includes correct design with security features, configuration, maintenance and management.

---

[163] David, W. Cybercrime, The Transformation of Crime in the information Age, Polity, (2007), p. 27.
[164] Misiko H (2014, July 30). How anonymous and other Hackitivists are waging war on Kenya. The Washington Post. Available www. post.com/news/worldviews/wp/. Accessed 20 February, 2018
[165] Hassan, A. B., Funmi, D.L., and Mikinde, J. Cybercrime in Nigeria: Causes, Effects and the way out. ARPN Journal of Science and Technology, 2(2012), pp. 626-631
[166] David, W. Cybercrime, The Transformation of Crime in the Information Age, Polity, (2007), p. 27.
[167] Ibid. p. 29

In Kenya, the emerging cyber threat trends are presented in the form of malware which is known to be a malicious software attack that causes harm to computer users and their system. The malware can manifest inform of viruses or worms that enter into the computer software without the user's knowledge. These attacks may include Botnet attacks, mobile malware attacks, phishing/password sniffing and Distribution Denial of Service (DDOS).

3.5.1 Botnet Attack

Botnet is described as a system of computers that have been penetrated and controlled by cyber criminals remotely. The botnets are presented in the form of malicious bots which are installed without the approval of the internet user. The botnets often remove the security hence exposing the computer user to risks which range from loss of personal data and increased vulnerability to fraud. According to Serianu (2014),[168] the growing number of fast internet connections, increases the chances of botnets attacks in Kenya. In 2013, cases of bonnets attacks detected grew by 100 percent from 900,000 events to 1,800,000 between the years 2012 to 2013.[169] This increase is attributed to the advancement in the internet connectivity coupled with unprotected computers which easily attract cyber criminals. The attackers take advantage of this situation to hack identified infrastructure such as financial institutions and government offices with a view to steal information (Serine 2014:12).[170]

It is noted that the attacks directed at various sectors of the economy vary from one to another. The Kenya banking sector has been the most targeted by the cybercriminals. According to a report by the Banking Fraud Investigations Department (BFID), report that about USD 300 million was stolen from bank accounts owned by individual customers in 2015 and 2016 out of which USD 10 million was

[168] Serianu, "Kenya Cyber Security Report, (2012).
[169] Serianu Ltd., "Kenya Cybersecurity Report 2014. Rethinking cyber security "An Integrated Approach: Process, Intelligence and Monitoring
[170] David, W. Cybercrime, the Transformation of Crime in the Information Age, Polity, (2007), p. 27.

recovered (Kamini 2011).[171] The BFID reports mentions theft of electronic based gadgets such as automatic transfer plate (ATM), electronic credit cards and other online frauds (KHRC, 2014).

The increasing innovations mobile banking services have exposed customers to new online vulnerabilities through malware and Trojan tools, (Serianu 2014).[172] Besides, the evolution of mobile banking technology in Africa and in particular Kenya, has provided a safe haven for criminals to perpetuate their crimes online by exploiting gaps in the weak security measures employed by financial institution and organization, (Serianu 2014).[173]

3.5.2 Malware Attacks

The malware is understood to be malicious software that is made up of worms, viruses and Trojan horses. It utilizes well known electronic communication devices to spread and includes worms sent through emails, text messages and text, infected files with virus downloaded from internet. Malware have been known to seek to make use of existing weaknesses for easy entry. According to a study conducted by Serianu in 2016, observed that the most common category in Kenya is the Worms which has affected 35% of all computers. The second most common category is the Miscellaneous Trojan which has affected which has affected 25% computers cleaned in Kenya.[174] The most known malware in Kenya is Win32/Autorun, which is a type that if of the family of worms that spread quickly copying itself to infected computer drive.

The only available and easiest way to militate against malware threats is to use intrusion detection system or antivirus that will help identify network traffic and conduct spot scans on abnormal

[171] Kamini, D. Cyber Crime in the Society: Problems and Preventions. Journal of Alternative perspectives in the Social Science, (2011), pp.240-259.
[172] Serianu, Kenya Cyber Security Report, (2014), p.7.
[173] Ibid, (2014), p. 9.
[174] Denial of Service Attacks" Cyber Security Engineering Team, Software Engineering Institute, Carnegie Melon University; URL: Available www.cert.org/tech_tips/denial_of|_service. Accessed 02 February, 2018.

communications. The prominence of this attack has been necessitated by the lack of use of antivirus to clean up the system. As Kenya continues to embrace online enabled services such as i-Tax System, Ken-Trade single window system and Integrated Financial Management Information System (IFMS), such as e-infrastructure have become susceptible to DDOs attacks (Serine 2014:11).[175] According to CSI Comp Crime Survey, (2010/2011) surveys malware attacks account for 67.1 per cent in Kenya cybercrimes.[176]

3.5.3 Mobile Malware Attack

According to MacAfee (2014), mobile malware is cited as a major driver of development in malware innovation and attacks in 2015. This type of attack was first reported in 2013 and targeted android platform which pointed at a growing mobile malware (MacAfee 2014).[177] Considering that over half of the population of Kenyan own mobile phones, mobile malware poses a substantial threat as they access internet services using their mobile phones. In the recent research carried out by "Kaspersky Lab and INTERPOL", Kenya was ranked third as a mobile malware risk state compared to Nigeria and South Africa (Matinde 2014).[178]

According to the CAK report of 2015/16, the number of malware attacks in the country was noted to exceed any other kind of cybercrime according to the annual report for the same period. It was reported that malware accounted for 80% of the attacks while web application accounted for about two percent of the cases reported.[179]

[175] David, W. Cyercrime, the Transformation of Crime in the Information Age, Polity, (2007), p. 27.
[176] "Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures" United Nations General Assembly resolution 64/211-2010.
[177] MacAfee 2014, MacAfee Labs Threats Reports. June wo14. Internet. Available www.macfee.com/hk/resourses//reports/rp-quarterly-threats-q1-2015.pdf.Accessed 5 Nov 2017
[178] Matinde, V. High Data Cost and Factors of Mobile Insecurity in Africa. IDG Connect, (2014), pp. 14-15.
[179] Communication Authority of Kenya (CA), Report 2015/16

3.5.4 Social Media Attacks

Social Media are links characterized by extremely cheap global mode of communication.[180] The platform has huge impact on social and security implications for the Kenya people and the government. Social media is an idiom used to refer to the group of technologies related to fast information distribution through net web-based platforms. It refers to broadcast media of multiple dialogues, featuring the Web 2.0 Internet revolution. "Web 2.0" represents an essential shift across the Internet use in the 21st century, which has transformed communication network where all users have the freedom to create and utilize the products.[181] Examples of Web 2.0 social media includes Facebook and Myspace, eBay reputation Flickr, YouTube, Google Maps and Twitter.

Social Media is a 21st century emerging communication technology that started in United States (US) and has spread exponentially to cover the entire world. According to 2010 report, Social Media users are estimated at over two billion people worldwide. Social media websites are most utilized websites by individuals and organization. The platform is now used to perpetrate crime in some parts of the world including Kenya (Serianu 2014).[182] These attacks present as defamatory hate speech, cyber bullying and terrorism.

3.5.5 Hate Speech

Hate speech is a complex nexus between freedom of expression and dignity. Hate speech is described as an expression that is intended to incite to harm by discrimination or advocate violence amongst persons or groups. It includes speech that threatens or inspires violent acts brought about by the growing internet

[180] MacAfee 2014, MacAfee Labs Threats Reports
[181] Chetty I and Basson A. Report on internet usage and the exposure of pornography to learners in South African schools Research report for the Film and Publication Board, Houghton, South Africa, (2006), p. 19.
[182] Symantec, "Internet Security Threat Report;" Serianu Ltd., "Kenya Cyber Security Report," 2012, Available at www. serianu.com/downloads/KenyaCyberSecurityReport2012.pdf. Accessed 09 March, 2017

use.[183] The cyber technology such as social media, website, email and blogs dominated by mobile telephony has been used to perpetuate hate speech that is now becoming a major cyber security threat in Kenya.[184] In accordance to "National Integration Cohesion Commission (NCIC), Act of 2008", hate speech is said to be the use of abusive, insulting words or cyber bullying which is aimed at causing hatred. The social media has been identified as a platform of communication of these abusive words which often seem to be founded on ethnicity.[185] Hate speech is a phenomenon that is on the increase which requires a framework regulate it.

According to reports of enquiries of the Kenya prior to election violence of 2007/2008, hate speech was rife in promoting negative ethnic incitements to violence among ethnic communities though to support certain contesting parties. During the inquiries, it was established that there was general high utilization of social media such as SMS and blogs were widely used to perpetuate the conflict. The Kriegler report on 2007/2008 elections, pointed to this emerging cyber technology of blogging community that fueled the violence.[186] This led to several political leaders arraigned for circulating speeches regarded to cause disharmony which is against the "National Cohesion and Integration Act 2008".[187]

[183] David, W. Cybercrime, the Transformation of Crime in the Information Age, Polity, (2007), p. 27.
[184] Alexis, O. SMSs used as a tool of hate in Kenya, (2016), p.92.
[185] Ibid, (2016), p. 94.
[186] The Commission of Inquiry on Post-Election Violence (Known as the Waki Commission after the Chairman of the Commission Justice Philip Waki) investigated the reasons for the violence and released its findings in a report known as the Waki report. See Waki Commission (2008) Ibid. Kriegler Commission (2008) Ibid. Kenyan National commission o Human Rights (2008) Ibid. Kriegle Commission (2008) Ibid. Kenyan National commission on Human Rights (2008) On the Brink of the Precipice: A Human rights Account of Kenya's Post-2007 election Violence: Available www.knchr.org/Portals/0/Reports/ KNCHR_REPORT_ON_THE_BRINK_OF_THE_PRECIPE.pdf. Accessed 13 September, 2017
[187] Kenyan National Commission on Human rights (2008) Ibid. Para 71, p29. See also Kriegler commission (2008) Ibid. p23.

3.5.6 Cyber Bullying

According to Kenya Computer Cybercrime Bill 2016, Cyber bullying is described as any transmission through a computer system intended to bully, intimidate or annoy the other person.[188] Cyber bullying or internet bullying are internet harassment terms that refer to aggression and violence committed through ICTs. These aggressions are concepts usually referred to as any injury that is deliberately and constantly inflicted on a specific individuals or groups.[189] Cyber bullying have become common in Kenya which utilize the use of emails that harass targets or posting of obscene photos and on social network sites which promote defamatory content. Similarly, Cyber intimidation in Kenya is a rising social challenge which many people are becoming victims (Serianu 2014).[190] The crime is perpetuated through mobile phones and takes the form of malicious text messages or pictures and videos of disturbing the content.[191] Crimes of this nature also include impersonation of persons and creating fake profiles with which to commit cyber aggression.[192]

3.5.7 Social Media and Terrorism

Kenya is a country that is considered a stable nation in the horn of Africa. However, recent events of terrorist attacks have put the country in the global map of war on terror after the US September 11, 2001 attack (Aranson, 2013).[193] The development in technology has given rise to a new era in terrorism where social media is used as a major stage of communication with wide variety of application including,

---

[188] Kenya's Computer and Cybercrimes Bill, (2016).

[189] William K, R. and Guerra N. G. Prevalence and Predictors of internet bullying. Journal of adolescent Health, 41, S14-S21, (2007), pp. 72-79.

[190] David, W. *Cybercrime, the Transformation of Crime in the Information Age*, Polity, (2007), p. 27.

[191] Marwick, A and Boyd, D. The Drama! Teen conflict, gossip, and bullying in networked publics. Draft version of paper to be submitted at the Oxford Internet Institute's 'A decade in internet time' symposium on the dynamics of the internet and society, (2011), p. 67.

[192] Aronson, S.L. Kenya and the Global War on Terror: Neglecting History and Geopolitics in approaches to Counterterrorism. African Journal of Criminology and Justice Studies: AJCJS, Vol.7, (2014), p. 94.

[193] Aronson, S.L. *Kenya and the Global War on Terror: Neglecting History and Geopolitics in Approaches to Counterterrorism.* African Journal of Criminology and Justice Studies: AJCJS, Vol.7, (2014), p. 94.

propaganda, planning and detonation of improvised explosives.[194] The Terrorist groups have used popular social networks such as Twitter, YouTube, Facebook and Flickr which offers exchange of short messages create for their communication purposes.[195]

The Al-Shabaab (AS) group has been in battle with Kenya since 2011 which led to Westgate and Garissa University attack in 2013 and 2015 respectively. The group has intensively used twitter account and has an estimated over 14,500 followers who are believed to include fighters in Syria and Yemen.[196] In 2014 Kenya witnessed an increased incidence of cyber attacks targeting both private and public institutions.[197] This phenomenon exposed the governent and private sector to security threats that are likely to effect the social political and economic sectors. Cyber-attacks are constantly evolving to an extent that the defenses are getting weaker each day. On July, 2014, cybercriminals hacked into Twitter account of the Kenya Defence Forces (KDF), and left a series of malicious tweets messages. The hackers were anonymous group who broke into the account of the force spokesperson and defaced the website. The attack on the defence forces account, has drawn attention to the potential threat of cyber-terrorism orchestrated by Somalia Al Shabaab and their ISIS outfit.

This scenario raises the question as to whether Kenya is prepared to counter cyber-terrorism and even deter or destroy the cyber-warfare capability of the cybercriminal.[198] The country's vulnerability to cyber felons arises from the large internet user base, estimated at over 25 million. According to scholars,

[194] Beate Stollberg, Tom de Groeve, The Use of Social Media within the Global Disaster Alert and Coordination System (GDACS), WWW– SWDM'12 Workshop April 16–20, 2012, Lyon, France, 2012.
[195] Dhiraj Murthy & Scott A. Longwell, Twitter and Disasters: The uses of Twitter during the 2010 Pakistan floods, may 2012
[196] Ibrahim, M. Somali and Global Terrorism: A Growing Connection? Journal of Contemporary African studies, Volume 28:3, (2010), pp.283-295
[197] Steele, Robert D. "Hackers and Crackers: Using and Abusing the Networks. "Presentation at the fourth Annual Conference on Computers, Freedom and privacy, Chicago, (1994), p. 70.
[198] Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., and Shitanda, S. Kenya Cyber Security Report 2015. Serianu Limited, (2015), p. 89.

Kenya is ranked position four in cyber-crime cases in Africa with leading nations such as Algeria Egypt and South Africa (Kagwanja & Karanja, 2014).[199]

3.5.8 Cyber Insider Fraud

Insider frauds emanate from lack of honesty among employees. While employees are expected to be honest, there are cases where some will be adamant to an extent that may undermine their employers. This is presented in a situation where an employee's attempts to misuse authority in a manner likely to compromise the security of the organization's daily operations of the business. On the other hand, cyber fraud is understood to be any misuse or falsification with a view to tampering with computer programs leading to losses sustained by the institution targeted. It involves the use of internet to perpetuate fraud through hacking, virus/worms' attacks, Dos attack amongst others. The fraud crimes include online stealing of cash, gambling and robbery. Cyber fraud is considered one of the main source of crime in Kenya where the government has identified it as among the highest cyber security threats. Mobile banking use has been named the most prone to attacks since over 1.7 trillion is transacted online (Wanjiku: 2013).[200] Kenya cyber frauds account for 22% of the economic crime reported. The major affected sector is the Kenyan banking institutions with cases of fraud have become prevalent (Business Daily, 2012).[201] According to "Kenya Banking Fraud Investigations Department (BFID)", the rise in the financial fraud is attributed to weak surveillance of ATM and reluctance to confront the fraud problem

[199] Kagwanja, P., and Karanja, M. (2014, August 18). How Cy-crime complicates war on terror. The East Aftica, Available www.theseastafrican.co.ke/news/How-cyber-crime-complicates-war-on-terror/2558-2422854-13ja90iz/index.html. Accessed 11 June 2018

Wanjiku, R. (2013). Kenya Banks face challenges with secure online transactions International banks are not as successful as in other markets. Available www.pcadvisor.co.ke/news/enterprise/3453739/ Kenyan-banks-face-challenges-with-secure-online-transactions. Accessed 23 July, 2017

[201] Daily Nation (2010). Kenya: Alarm as bank employee's siphon out Sh2.4bn through "inside jobs." 20th July 2010 Available at www. allafrica.com/stories/201007120388.htm. Accessed February, 2018

caused by internet technology, (Technology Banker, 2012).[202] The BFID report show that about USD 27.52 million from customer's bank accounts was stolen in 2015 and 2016 with only USD 10 million recovered (BFID, 2013).[203] The report cited electronic funds transfer, credit card theft, documents forgery and online frauds as key methods utilized.

The increasing online banking innovations have equally increase vulnerabilities to customers especially from local banking institution to the emerging cyber threats. In the circumstance, online and mobile banking frauds are executed by misleading the users by interfering with their login data using malware tools and Trojan (Serianu, 2014).[204] Additionally, financial institutions have been reluctant to report such frauds, while courts have remained insensible in the prosecution of perpetrators.

3.5.9 Cyber Stalking

According to Ovidio and Doyle, 2003, cyber stalking is described (Yar, 2006) as a persistent harassment targeted at individuals through use Internet and web related digital strategies intended to upset, intimidate a person.[205] Cyber stalking is a form of online oppression which is significantly unique as compared to off-line stalking. The resemblances are on the nature of attacks which target women from their counter male stalkers.

3.6.0 Cyber and Elections

Cyber technology has been reported to be used to manipulate election results as was recently alleged on United Sates (US) Donald Trump's elections. According to Illinois investigators, there is confirmation that cyber attackers from Russia attempted to erase or modify voter data bases and software systems.

[202] Technology Banker. (2012). Fraud Solutions for Africa Banks: A Kenyan Perspective. Available at www.tecnologybanker.com/security-risk-management/fraud-solutions-for-africa-banks-a-kenyan-perspective. Accessed 13 May, 2018
[203] Bank Supervision report, 2013. Annual Report, Central Bank of Kenya
[204] David, W. Cybercrime, the Transformation of Crime in the Information Age, Polity, (2007), p. 27.
[205] D'Ovidio, R & Doyle, J. A Study on Cyberstalking: Understanding Investigative Hurdles, FBI law enforcement bulletin, (2003), p. 8.

The alleged hackers' accessed software intended to be used by election workers on the day of elections including campaign finance database. Similarly, in the August 2017 elections, Kenyan opposition National Super Alliance (NASA), and alleged hacker's manipulation into Kenya's electoral commission database which led to the nullification of results and elections repeated.

3.7 CHAPTER DATA PRESENTATION, INTERPRETATION AND ANALYSIS

To better understand the emerging patterns of cyber technology as a threat to national security, data was collected from professionals in ICT organizations and institutions in Kenya. The study targeted a population of 75 and obtained a sample of 50 representing 66.7 percent of the population as shown in **Table 3.1** below, which is acceptable as agreed by Borg and Gall.[206]

Table 3.1 Response Rate

SER	ORGANIZATIONS	POPULATION	SAMPLE SIZE	PERCENTAGE
1	Ministry of Foreign Affairs, Kenya	7	5	
2	Ministry of Devolution	3	2	
3	Communication Authority of Kenya	4	-	
4	Kenya Revenue Authority	4	1	
5	Banks (Kcb & Coop Bank Nairobi)	5	5	
6	Diplomats (Botswana And Somalia)	4	4	
7	Advocated (Asa & Asa Adv)	7	2	
8	Universities – UoN, USIU & Tech Univ of Nairobi	3	3	
9	Kenya Defence Forces Headquarters	5	5	
10	National Police Service	3	3	

[206] Borg, R. and Gall, D. Education Research. 6th Edition. New York Longman Inc (1996), p. 17.

	Headquarters			
11	National Intelligence Service Headquarters	3	3	
12	Safaricom	4	-	
13	ICT Business Organizations (Interfina House Nairobi)	8	7	
14	Others (Cyber Café Nairobi)	15	10	
TOTAL		**75**	**50**	**67%**

Source: Author (2018)

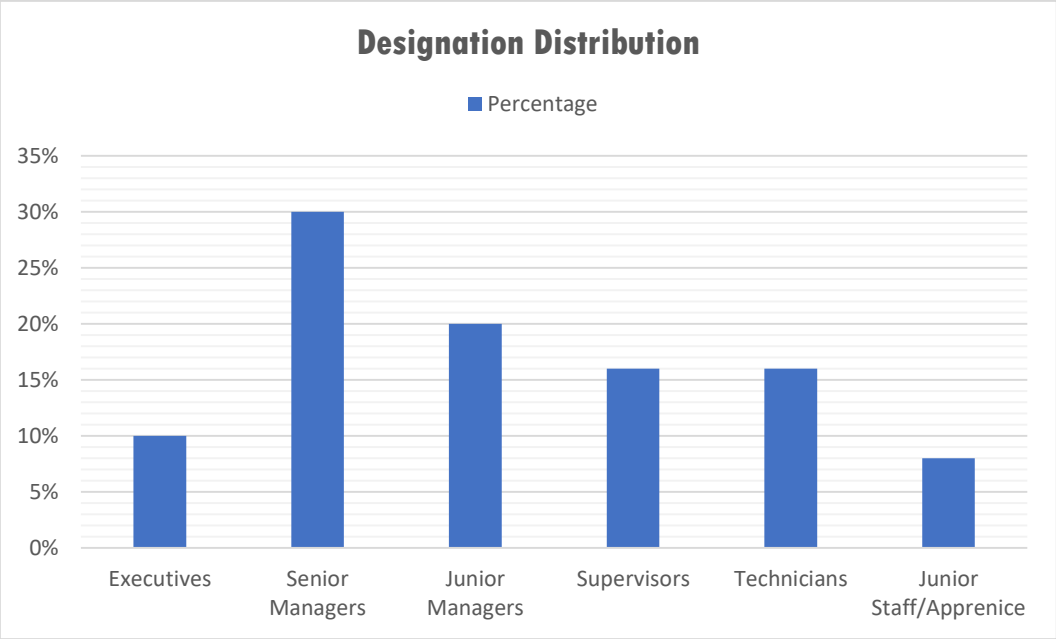
3.7.1 Designation Distribution

From the data, majority of the respondents were senior managers at 30%, junior managers at 20% and supervisors, technicians and junior staff at below 16%. Table 3.2 and Fig 3.1 below shows a fair representation across the management and supervisory levels of the institutions suggesting that the ICT department is well managed by professional senior staff. Based on this data the study is likely to receive higher chances of well informed and quality information from the respondents thereby increasing the validity of the study.

Table 3.2: Designation Distribution

Designation (ICT)	**Frequency**	**Percentage (%)**
Executives	5	10
Senior managers	15	30
Junior managers	10	20
Supervisors	8	16
Technicians	8	16
Junior staff/apprentice	4	8
Total	**50**	**100**

Figure 3.1: Designation Distribution



Source: Author (2018)

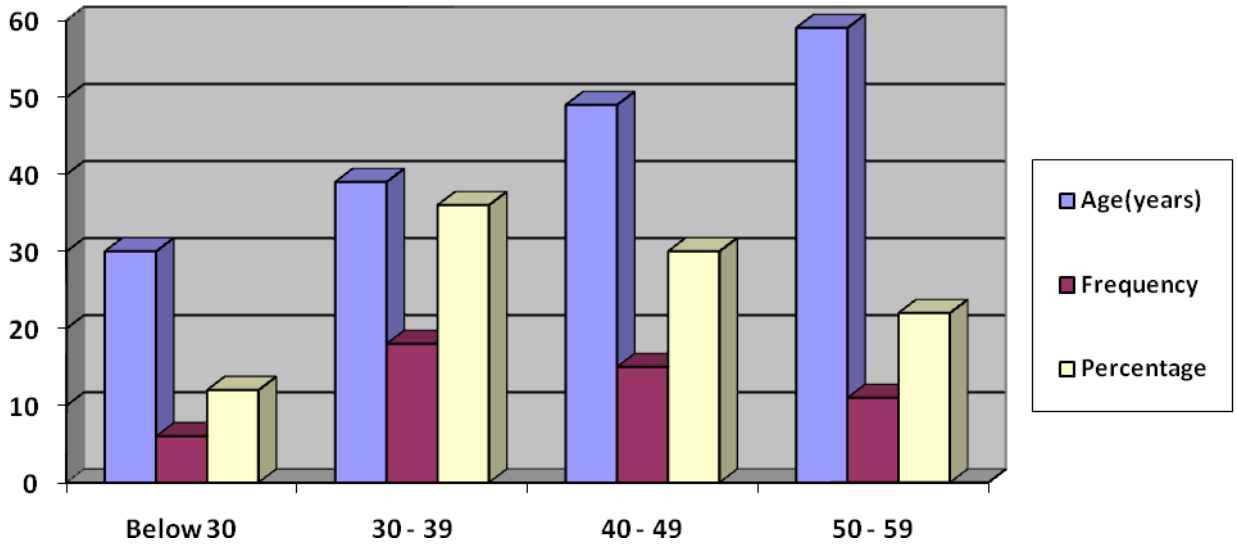
3.7.2 Age Distribution

The age distribution of the respondents was sampled in groups of nine years' interval. The results were that 12 percent were below the age of 30 years, 36 percent were in the ages of 30-39 years, 30 percent were in the ages of 40-49 years and 22 percent were also in the ages of 50-59 years as shown in Table 3.2 and Fig 3.1 respectively. This shows that the ICT department is managed by fairly aged senior staff of between 30 to 50 years of age. This also shows the level of maturity and experience that helps to meaningfully contribute to the study.

Table 3.3: Age Distribution

Age (years)	Frequency	Percentage (%)
Below 30	6	12
30 – 39	18	36
40 – 49	15	30
50 – 59	11	22
Total	**50**	**100**

Figure 3.2: Age Distribution

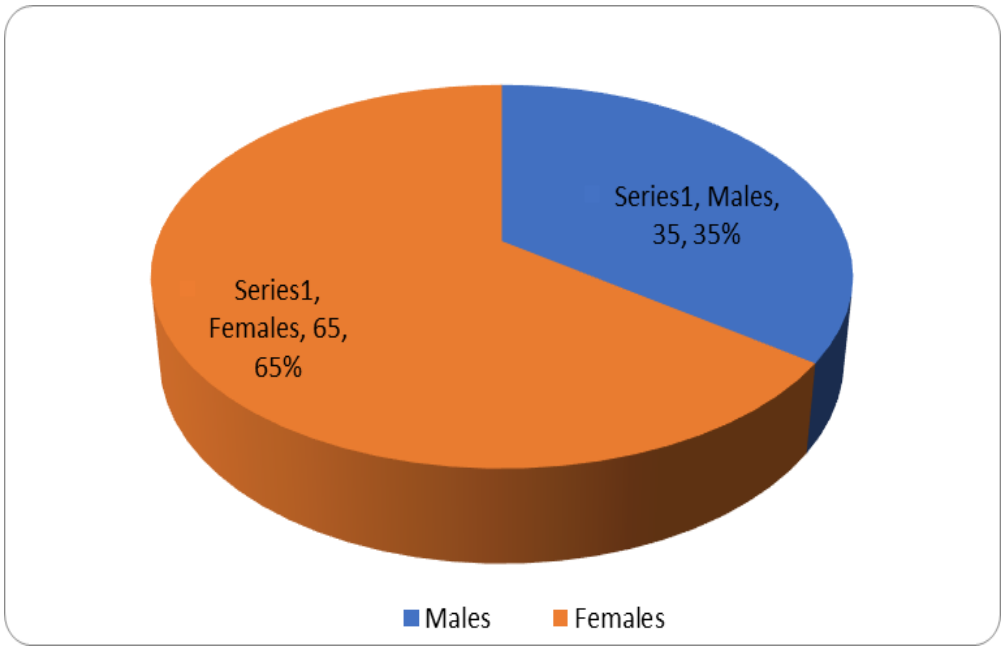


Source: Author (2018)

3.7.3 Gender Distribution

The gender distribution of the respondents was made and 65 percent were male while 35 percent female as shown in Pie Chart 3.1. This shows that the ICT sector is well represented with over 30 percent gender distribution as required in the Kenya Constitution, 2010. This shows a balanced representation which improves the reliability of findings.

Pie Chart 3.1: Gender Distribution



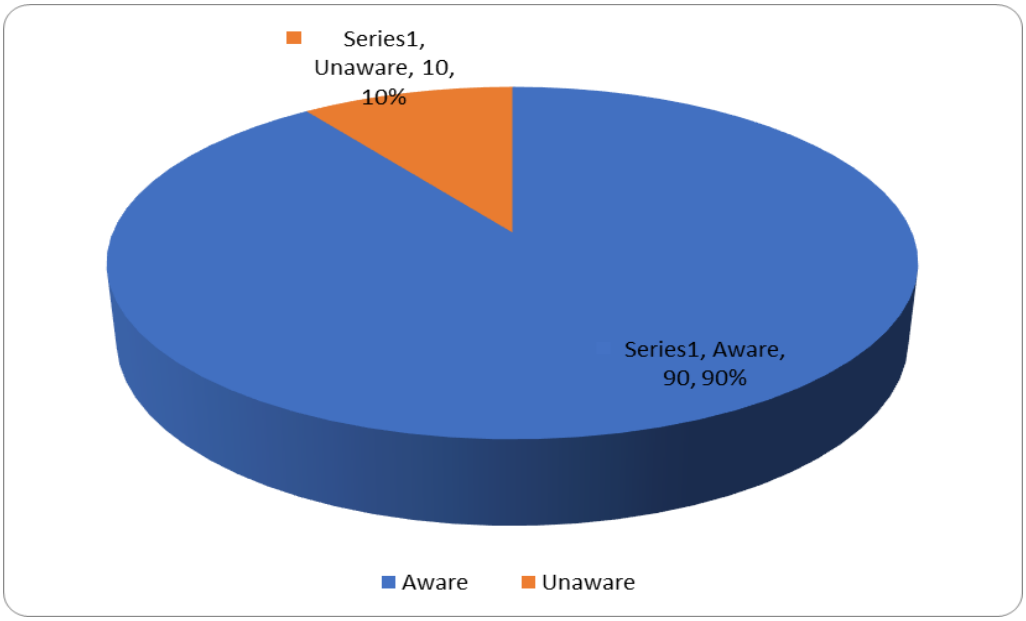
Source: Author (2018)

3.7.4 Knowledge on Cyber Threats

As shown in the literature paragraph 3.3 to 3.5, the emerging threats of cyber technology in Kenya have always favoured the attackers. This study sought to determine the respondents' knowledge of cyber threat awareness in the work place. From the data 90 percent agreed that they understood cyber threats while 10 percent were unaware as shown in Pie Chart 3.2. These results suggest that majority of the

respondents were aware of the threat and therefore can successfully respond to any attack. The few who were unaware may likely be the apprentice junior staff on training. This implies that there is need to create awareness amongst this staff to regularly check the network and clean the system in order to avoid a likelihood of attacks.

Pie Chart 3.2: Knowledge on Cyber Threats



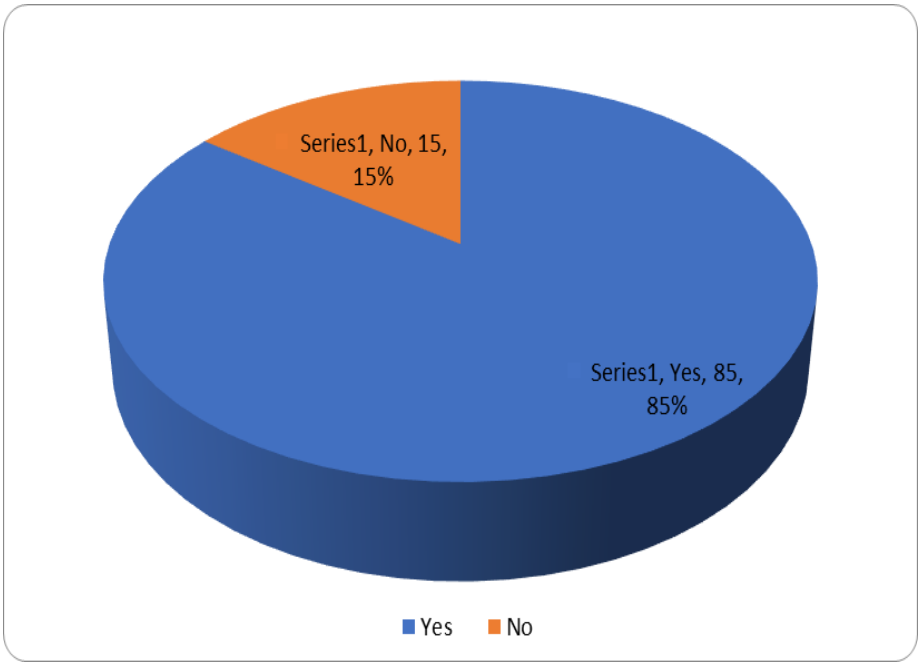
Source: Author (2018)

3.7.5 Experienced Cyber Attack

With the increased rate of cybercrime in Kenya, this study sought to establish if respondents had experienced any form of cyber-attack in their work place. The findings revealed that 85% Agreed that they had experienced malware, botnets, Trojan worm while 15% were Undecided. This result reveals gaps in institutional awareness of cyber threats and the overall information security. It may also point at a purely implementation of regulations with respect to enhancing cyber security at institutional level as shown in Pie Chart 3.3 and Table 3.4 below. In view of this institutions need to invest in computer

intrusion detection systems to avoid attacks from malware and other malicious communication. In addition, there is need to build capacity in reinforcing operating systems to improve the ability to withstand attacks.

Pie chart 3.3: Experienced Cyber Attack



Source: Author (2018)

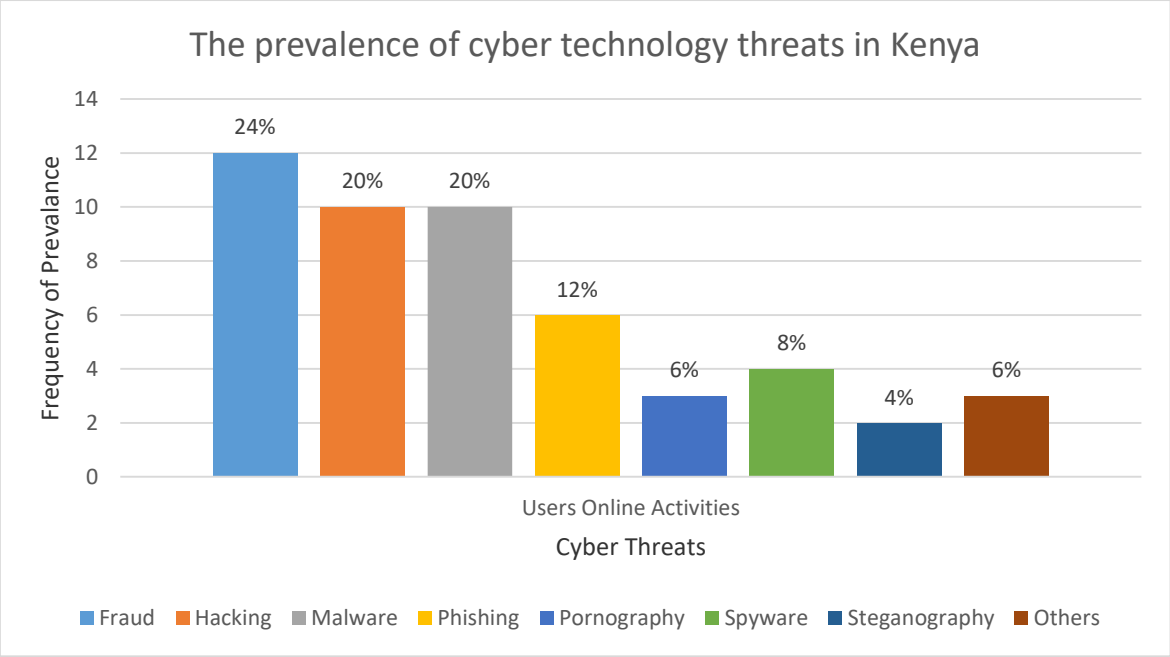
3.7.6 The Prevalence of Cyber Technology Threats in Kenya

The study sought to establish knowledge on the common type of cyber-attack that they most experience. According to the study, most of the respondents identified cyber fraud as the most prevalent at (24%), hacking and malware at (20%), phishing (12%), spyware at (8%), Phonography (6%), Steganography (6%) and others (6%) as shown in Table 3.4 and Fig 3.3 respectively. The unanimous agreement suggested by these results was further supported by the sentiments expressed by interviewees who explained that the threats were many and come from any part of the world. This agrees with literature in paragraph 3.5 above.

Table 3.4: The prevalence of cyber technology threats in Kenya

Type of cyber attack	**Frequency**	**Percentage (%)**
Fraud	12	24
Hacking	10	20
Malware	10	20
Phishing	6	12
Pornography	3	6
Spyware	4	8
Steganography	2	4
Others	3	6
Total	**50**	**100**

Figure 3.3: The prevalence of cyber technology threats in Kenya

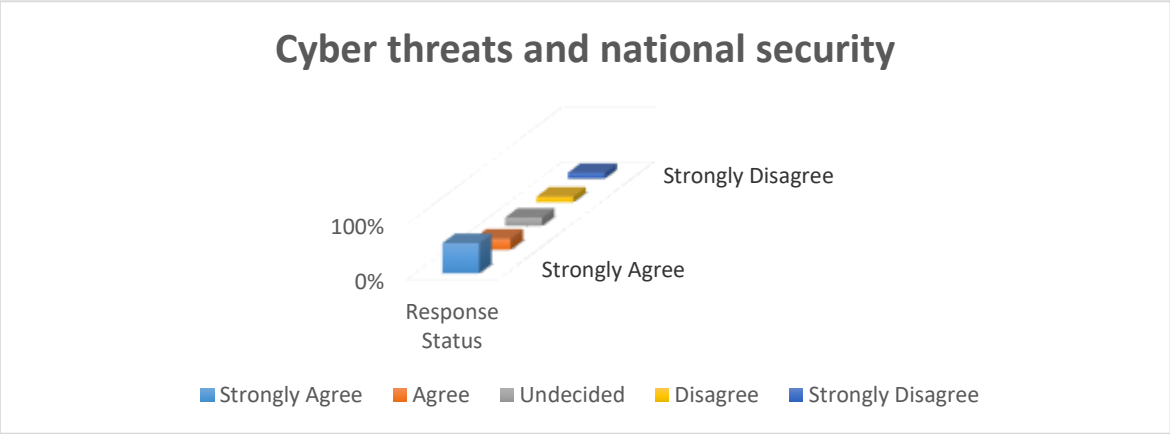


Source: Author (2018)

3.7.7 Cyber Threats and National Security

This research sought to determine if cyber insecurity has a direct influence on a national security. The outcome showed that 55% strongly agreed, 20% Agreed, 15% were undecided and 10% disagreed as shown in Figure 3.4. From field study, the respondents from the security sector such as Kenya Defence Forces (KDF), National Police Service (NPS), National Intelligence Service (NIS) and the Banks positively related the threats to national security. The respondents who agreed could not elaborate how it was precisely linked to security of the nation. This helped to validate the reliability of findings on the existing literature research gap in section 1.7.1.

Figure 3.4: Cyber threats and national security



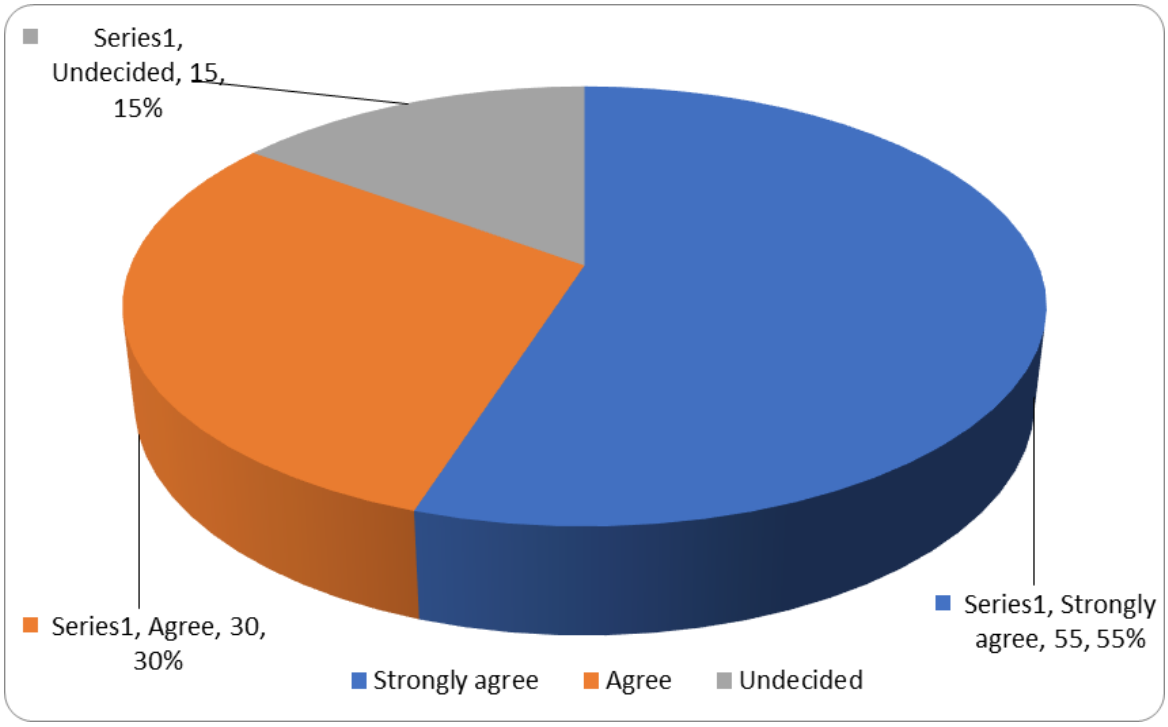
Source: Author (2018)

3.7.8 Increased Cyber Threats Prevalence

The respondents were asked to conform if cyber threats rate were on increase in their organizations. From the findings most of the respondents acknowledged that they have experienced increased cyber

threats in the last two years with 55% strongly agreed, 30% agreed and 15% were undecided (15%) as shown in Pie Chart 3.4.

Pie chart 3.4: Cyber threat prevalence



Source: Author (2018)

The increase in the attacks may be related to the need to commit financial fraud, access confidential information in order to gain comparative advantage, out of malice or increased crime. This validates the research on why Kenya cyber infrastructure remains vulnerable.

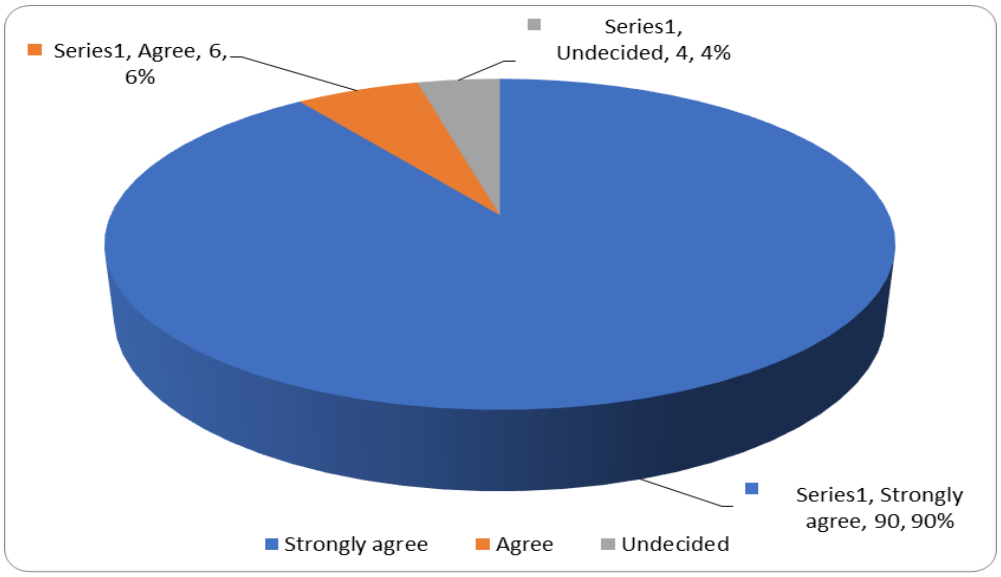
3.7.9 Drivers of Cyber Attack

The research sought to find out what drives criminals to commits cybercrimes. From the findings, the respondents identified financial frauds, access to confidential information, malice, fun, cyber warfare and espionage with 90% strongly agreed, 6% agreed and 4% were undecided as shown in Pie chart 5.6. From the results it shows that there are weaknesses in the cyber security measures which the attackers

are exploiting. This is likely to shows that most institutions lack practical guidance coupled with poor implementation of cyber security controls.

The findings agree with Siegel, *et, al*., who stated that most of the shared common computer frauds include computer operations where insubstantial resources are epitomized in data form such as money transactions are lucrative targets of fraud related to computers. The results were also in line with Kenya Cyber Security Report, (2016) that state that cybercrime target Government offices, banking institutions, financial services and mobile money sector. This validates the research to identify drivers of cyber-attacks and the institutions preparedness.

Pie chart 3.5: Drivers of Cyber Attack



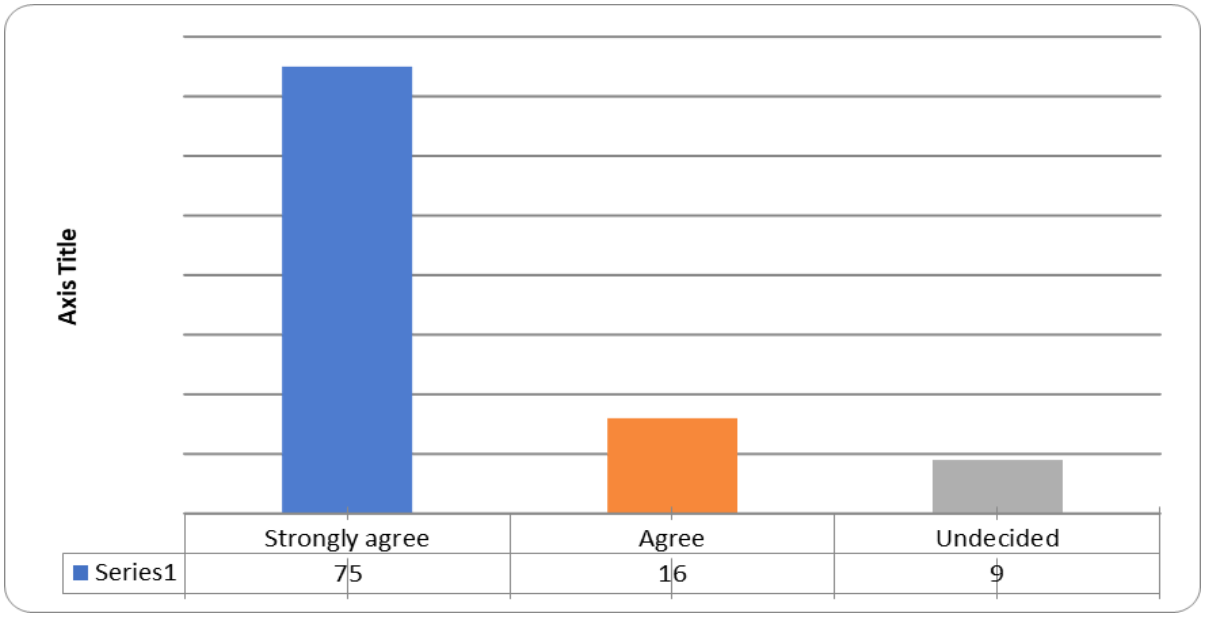
Source: Author (2018)

3.8.0 Patterns of cyber technology and Security threats

This study noted that while cyber security was a global responsibly, taking cognisance of the increasing technology, it sought to determine the patterns of cyber technology and its effects on security. The

outcome was that 75% Strongly Agreed, 16% Agreed while 9% were Undecided as shown in **Bar Chart 3.5**. This helped to improve the reliability of findings.

Bar chart 3.5: Patterns of cyber technology and Security threats



Source: Author (2018)

3.9 Summary of the Chapter

Cyber-attacks in Kenya have developed to be prevalent and more serious to national security due to its porous nature and complexity. This is because of the upsurge in computers applications across the sectors of the economy which has attracted criminals aiming to exploit the opportunities available. As shown in the trends of threats presented and the field data, the attacks have also become increasingly sophisticated because of the asymmetric nature of operations. Whereas, there are measures in place to protect the infrastructure, there still exists a huge gap that needs immediate action to protect ICT environment. Kenya must therefore invest in implementing new approaches that will protect the infrastructure as threats and business processes change.

CHAPTER FOUR

AN EVALUATION OF CYBER SECURITY MEASURES AND STRATEGIES APPLIED IN KENYA

4.0 Introduction

This study examines the strategies that Kenya has laid to address the increasing cyber-security threats as it embraces e-governance and e-commerce strategies in its economy. The study explores the measures and strategies applied in Kenya to safeguard the ICT sector against cyber threats. The measures include developing cyber capacity and national institutions to provide a secure and safe cyber environment. The chapter also presents analysis of the findings from the field in relations to the objective under study.

4.1 Kenya Cyber Security Resilience

Kenya has ambitiously emerged as EAC leading ICT manager in the region and has made progress in integrating ICTs into most sectors of the industry. For the last decade, the ICT sector has witnessed incredible progress in the area of socioeconomic development.[207] This trend has been supported by market liberalization and improved by new technologies and subsequent innovations. The Government has recognized and integrated the ICT to the national development objectives as a strategy to achieve Vision 2030.[208] The ICT infrastructure has been included in public policy as a tool to improve the livelihood of Kenyans through provision of affordable services.[209]

The debate on cyber security in Kenya tends to concentrated around cases of hacking, insider frauds, botnets, Trojan worms, sensitive information leaks and infectious malware. However, little consideration has been given to matters relating to cyber resilience efforts to address emerging and

[207] Seniaru, (2016).
[208] Kenya Vision 2030, Available www. vision2030@kenya.go.ke. Accessed 10 April 2017.
[209] Maina, E. A survey on impact of ICT on Business Value Creation in Kenya Banking Sector. Unpublished MBA project, University of Nairobi, (2010), p.7.

unexpected threats in the cyberspace. The word resilience refers to the efforts put to encourage implementation of whole measures that will ensure that the system remain operational in the event of failure in an attack. The purpose is to maintain normal services when the system is threatened with an attack.[210]

The conception of cyber resilience in Kenya underscores the need for coordinated approach to cyber security incidents, and the corresponding measures to contain cyber in-security. These efforts have often been discriminating and motivated by narrow agendas perpetrated by the Western powers with interest in Africa. These powers have leaned on their agenda mainly aimed at combating fanaticism (Cassim 2011).[211] The United States of America (USA) efforts in some African countries especially Kenya, have helped build capacity cyber-attack preparedness as a component of wider counter terrorism approach, as opposed to the cyber security efforts for the region.

4.2 Strategies to Address Cybercrime

In 2013, Kenya realized that ICT contributed about 12.1 percent of Kenya's GDP (Mwenesi, 2014a).[212] These programme were largely supported by World Bank Group which devoted US$4.1 billion for a number of years between 2010 and 2003 (Mwenesi 2014b).[213] The Kenya Cyber Security Policy is presently coordinated by Communication Authority of Kenya.[214] Key tenets of the policy are

[210] Kigen, et al, 2014, "Kenya Cybersecurity Report 2014."Available www. serianu.com/downloads/KenyaCyberSecurityReport2014. Accessed 28 July, 2018
[211] Cassim, F. 2011. "Addressing the Growing Specter of Cybercrime in Africa: Evaluating Measures Adopted by South Africa and other Regional Role Players." Comparative and International Law and Justice South Africa 44:123-38.
[212] Mwenesi, S. ICT Contribution to Kenya's GDP now at 12.1 percent. Human IPO, July 22. Available www.humanipo.Com/news/46203/ict-contribution-to-kenyas-gdpnow-at-12-1. (2014), p. 19. Accessed 10 March 2018
[213] David, W. *Cybercrime, the Transformation of Crime in the Information Age*, Polity, (2007), p. 27.
[214] Paula, K., Carol, M., Kevin, K., Martin, M., & Barbara, S. (2014). Kenya Cyber Security Report 2014. Nairobi.

computer access training and awareness, cyber safeguards and policies ICT economic drivers, ICT Governance and Legal framework.[215]

Through these strategies several teams have been established to oversee implementation of cyber technology and security measures as anchored in the law. 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.[216] Despite these efforts, in 2014 the country faced one of the major international cybercrime cases which have exposed existing cyber weaknesses and gaps in the infrastructure.

4.3 Kenya Cyber Security Policy Framework

Kenya holds a leading ICT position in East Africa, has made efforts to incorporate ICT into various subdivisions of the economy.[217] The ICT segment in 2013 contributed about 12.1% of Kenya's GDP (Mwenesi 2014a).[218] On the basis of this development record, World Bank Group between, 2003 to 2013 invested US$4.1 billion on ICT, (Mwenesi 2014b).[219] Such expressions presented enormous opportunities in Kenya's ICT sector, pointing out at a need to focus more on tackling emerging challenges of cyber threats.

Kenya's first witnessed a major cybercrime in 2014, which exposed the country's cyber security gaps. The case of foreigners from Thailand's and Chinese in 2014 who were arrested attempting to infiltrate Safaricom M-PESA (Mobile Money Transfer) system, Automatic Teller Machines (ATM) and

[215] Communication, connected Kenya, (2017). Retrieved 11, 13, and 15, from ICT Authority: http://ww.ict.go.ke/doc/MasterPlan2017.pdf. Accessed 20 December, 2017
[216]Communications Authority of Kenya. (2015). First quarter sector statistics report for the financial year 2015/2016. Accessed 03 Feb 2018.
[217] Communications Authority of Kenya. (2015). First quarter sector statistics report for the financial year 2015/2016. Accessed 03 Feb 2018.
[218] Mwenesi, S. 2014a. "ICT Contribution to Kenya's GDP now at 12.1%. Human IPO, July 22 Available www.humanipo.com/news/46203/ict-contribution-to-kenyas-gdp-now-at-12-1/. Accessed on 08 May, 2018
[219] Ibid p.10

bank accounts exposed the cybercrime ring operating in the country, (Agence France-Presse 2014).[220] This revelation strengthened Kenya's resilience to remain as a leading player in ICT while seeking to cooperate with other actors who have developed infrastructures to respond to such emerging threats.[221]

With the assistance of ITU support in 2012, the Government established an agency known as the Kenya National Computer Incident Response Team Coordination Centre (KE-CIRT/CC) to coordinate issues related to cyber security management. The KE-CIRT/CC was specifically to advice on national cyber-security preparedness in coordination with other stakeholders at local, regional and international level. The centre reports to the CAK and is responsible for technical advice and research and development in cyber threats. However, the centre has remained docile and has not been of help to the nation.[222]

Given the recent reported cases of fraud through cyber technology in Kenya, the question remains if this institution will ever produce required results. The Kenyan case points at a lack of practical knowledge and therefore showing the need to move from speculation to practice in order to strengthen the existing cyber security institutions.

4.4 Cyber Security Strategy Plan

The Kenya National Cyber Security Master Plan 2017/2018, is a strategy document that has been developed to address the risks that ICT is likely to face in future. The Strategy is built on the three pillars of Vision 2030 which defines Kenya's cyber security and objectives to be achieved in order to secure a safe cyberspace, while promoting ICT to an enabler to economic growth. This has been achieved by enacting Kenya Information and Communication Act (KIC), Cap 411A which is an

[220] Gagliardone, I. Media Development with Chinese Characteristics." Global Media Journal, Government of Kenya. 2014. Cybersecurity Strategy. Ministry of Information Communication and Technology, (2014), p.6.
[221] Akamai, the State of the Internet. Available,www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-connectivity-report.pdf. Accessed 12 May, 2018.
[222] ITU. 2015. ICT Statistics. Available www.itu.int/en/ITU-D/ Statistics/Pages/stat/default.aspx. Accessed 8 February 2017

amendment to ICT ACT, 2014 and establishes a National Certification Authority Framework (NCAF), aimed at providing a foundation for partnership with key regional and international on cyber security. This includes opportunities such as ITU and East Africa Communications Organization (EACO).[223] The national strategy will assist in making Kenya improve the current cyber security posture and provide guidance on how to secure cyber infrastructure against emerging threats. This will only be if there exists a strong cyber security doctrine reinforced with policy, legal and regulatory framework.[224]

In addition, the government has accepted the need to establish a Cyber Coordination Centre where all cases of attack on critical ICT infrastructure can be reported. The center is established under CAK and is intended to respond to any online attacks or threats to security in the country.[225] Further, the Computer and Cybercrimes Bill of 2016 which seeks to bring into line the law to developing forensic procedures when investigating increasing cases of cybercrimes is yet to be actualized.[226]

4.4.1 Legal Framework

According to the second edition of Global Cyber Security Index report 2016, Kenya is ranked amongst the top three African countries committed to cyber security measures.[227] In the newly established Kenya Cyber Security Policy 2016, all cyber threats are coordinated by the Communication Authority of Kenya.[228] Key tenets of the policy are computer access training and awareness, cyber safeguards and policies ICT economic drivers, ICT Governance and Legal framework.[229] Through these strategies several committees have been formed to watch over the implementation of cyber technology and

[223] Gagliardone, I., and Sambuli N. Cyber Security and Cyber Resilience in East Africa. Centre for International Governance Innovation, (2015), p. 234.
[224] Fischer, E. Creating a National Framework for Cyber security: An analysis of Issues and Options, February 22, CRS Report for congress, Order Code RL3, (2015), p.2777.
[225] The East African, Kenya Launches Centre to fight cybercrime, (2016).
[226] Government of Kenya. 2014. Cybersecurity Strategy. Ministry of Information Communications and Technology.
[227] Global Cybersecurity Index GCI, (2017), p. 10.
[228] Paula, K., Carol, M., Kevin, K., Martin, M., & Barbara, S. (2014). Kenya Cyber Security Report 2014. Nairobi.
[229] Communication, K. I. (2013). Connected Kenya 2017. Retrieved 11, 13, and 15 from ICT Authority: Http://www.ict.go.ke/docs/MasterPlan2017.pdf. Accessed 25 January, 2018.

security measures as anchored in the law. Recognizing the importance of ICT, the Office of Directorate of Public Prosecutor (ODPP) has branch devoted to cyber security crimes under the law.

4.4.2 Cyber security Laws

Kenya has several cyber security laws which includes: "The Kenya Information and Communications (Amendment) Act (Cap 411)"[230] and "The Proceeds of Crime and Anti Money Laundering Act, No. 9 of 2009" among others. Other cyber security policies and regulations that have been amended include "Computer and Cybercrime Bill (2016)", "Cyber Security Regulations (2016)", "Cyber Security and Protection Bill (2016)" amongst others. These new bills are likely to affect old laws and improve cyber security management.

4.4.3 ICT Act 2013

"Kenya Information Communication Amendment Act 2013" - this includes Data Protection Bill (2013); introduces Cyber Security, e-Commerce and Broadcasting legislations. It aims at developing safe and sound environment for the cyber space by promoting and facilitating efficient management of critical internet resources.[231]

4.4.4 CAK (Cyber security)

The regulation of 2016 is envisaged to develop a framework that will facilitate the investigation and prosecution of cyber technology crimes and offences. It also aims to facilitate electronic commerce and

[230] Part VIA, Kenya Information and Communication Act (Cap 411A)
[231] Foreword, Kenya Information and Communications (Amendment) Act, (2013).

eliminate barriers to e-commerce and e-leadership. It seeks to define Offenses and Penalties in case of breaches.[232]

4.4.5 National Cyber Security Strategy 2017/18

This aims at promoting the Government's pledge to cyber security. The Strategy includes the following goals: To enhance the cyber security in order to encourages ICT e-business environment and eliminate vulnerabilities. To build cyber security awareness in order to develop competent workforce to address cyber security needs. This will be realized through training and sensitization workshops and other forums. In order to augment collaboration and information sharing among relevant stakeholders and this will be accomplished through the established regional organizations and stakeholder's meetings. To develop national ICT leadership to develop cyber security strategies and legal frameworks at all levels.

4.5 Sector Cyber Security Measures

This part will focus on a few institutions to check of the measures and strategies in place to address cyber-security challenges.

4.5.1 Kenya Banking Sector

The Central Bank of Kenya (CBK) under Section 33(4) of the Banking Act, has issued cyber security guidelines that will help banks deal with cybercrimes and prepare for emerging threats.[233] The Guidance Note outlines the minimum requirements that institutions must take to protect against cyber-attacks. The guide helps to create a secure and safe cyberspace that underpins information system security in the Kenyan banking sector. It places responsibility for protection of the institutions business to the line

[232] Section 3, Draft Cybercrime Bill of Kenya (2014).
[233] Central Bank of Kenya governor Patrick Njoroge during the Monetary Policy Meeting in Nairobi held aimid backdrop of improved weather conditions on May, 2017

managers. It encourages all staff to implement IT security awareness training programmes and guide on best practice performance.[234] The Information Communication Technology Association of Kenya (ICTAK) has also offered to assist banks strengthen this regulation in order to combat cybercrimes.[235]

4.5.2 Mobile Service Providers (Safaricom)

Safaricom maintains a state-of-art information technology (IT) security system which automatically activates an alarm if breaches are detected. The company experiences over 17million cyber security threats per day. The company has succeeded to monitor cybercriminals through partnerships with CAK, National Police Service (NPS), National Intelligence Service (NIS) and other international networks such as Vodafone, which give real time information on possible threats and in responding to other cyber technology threats emanating from other countries. Through a sustained surveillance and a multiple layers defence system through a chain of command that involves the maker, checker and authorizer of the system, Safaricom has been able to easily track any breaches.[236] Safaricom holds the world commended ISO 27001 Information Security Management System Certification which confirms adherence to appropriate processes and controls in the industry.[237]

4.5.3 Kenya Revenue Authority (KRA)

Kenya Revenue Authority has experienced an increase in cyber-attacks owing to security breaches obviously highlighting new challenges facing the society. The Kenya Revenue Authority (KRA) was

[234] Central Bank of Kenya GUIDANCE NOTE ON CYBERSECURITY, 2017
[235] Wechuli A. (2014) on Cyber Security Assessment Framework: Case of Government Ministries in Kenya; International Journal of Technology in computer science and Engineering, 1(3).
[236] Biztech Africa. (2011, October 29). Safaricom unveils cloud deployment. Available www.biztechafrica.com/section/internet/article/safaricom-unveils-largestnative-cloud-deployment-/1365/. Accessed 03 January, 2018.
[237] Kemibaro, M. (2011, October). Safaricom CLOUD: Safaricaom's third act to dominate Kenya's telecoms sector? Available www.moseskemibaro.com/2011/10/29/safaricomcloud-safaricoms-thirdact-to dominate-Kenya's-telecoms-sector./ Accessed 05 January, 2018.

established under the Act of Parliament, Chapter 469 of 1995 laws of Kenya. It is responsible for revenue collection through e-government system (KRA, 2011).[238] This system has been susceptible to cyber-attacks and KRA has embarked on user awareness training, use of safeguards such as antivirus and strict adherence of company policies on internet access.[239]

4.5.4 Academic Sector

The academia plays an important position in strengthening cyber security by engaging on Research and Development (R&D). Kenya lacks behind in the investment on R&D and hence our development rate is very low. The e-learning programme that has been introduced is likely to be source of cybercrime unless measures are put in place to regulate the system. Noting that the learning highly relies on internet, the programme is likely to be confronted with cyber security challenges as a consequence of illegal activities the learners may engage in. As e-Learning systems are challenged by an open and interconnected distribution and hence delivering a secure environment may be a challenge that the government will need to grabble on.[240]

4.6 Opportunities

Despite the many obstacles that undermine the protection of cyber technology during counter cyber security measures, on the flip side, there are also opportunities that if exploited can improve cyber technology and in-security nexus.[241] Finding a good balance that provides for both technology and security rights without compromising on any one of them guarantees the enjoyment of both. As

[238] KRA. (2011). KRA Online Service. Available www.kra.go.ke/index.php/kra-portal.Accessed 14 March, 2018
[239] Alsmadi, I. (2011, December). Security Challenges for expanding E-governments' Services. International Journal of advanced Science and Technology, 37, 47.
[240] Bandara, I. Ioras, K. Maher, C. Lusuardi – Cyber Security Challenges of Distributed e-Leraning System, (2015), P. 219
[241] Thorpe, P. 1984. The impact of new information technology in the developing countries. Journal of Information Science, Vol.8, no.5

Hoffman argues, an attempt to trade human rights for security, quite often, one ends up with neither.[242] Embedding this approach as part of national security strategy can ensure a more sustainable way in addressing the causes of cyber insecurity.

4.7 Cooperation

Countering cyber security efforts provide an opportunity for both bilateral and multilateral cooperation between states and between states and other organizations that may be involved in the war against cyber threats such as ITU, International CERTs agencies, AU, EAC regional organizations and others.[243] Due to the transnational nature of cybercrime, working with other states to monitor the trends of cyber threats across the borders can aid in disrupting and pre-empting the threats. In certain instances, it can also help in interdicting sources of funding of cyber criminals. Quite often, cybercrime is funded by a sponsor individual or organization whom in most of the times is domiciled in another state.[244]

The Kenya government can cooperate with other states over a set of diplomatic and security issues in the country and in the region, that, if addressed effectively, can serve to mitigate the cyber threats in the country and the entire region. While the lack of active engagement of the developed countries to fight cyber threats in developing nations of Africa can be understood, failure to establish a stable and functional cyber authority in Africa continues to provide a fertile ground for cybercriminals from where they undertake they undertake their criminal activities and thereby destabilizing the entire

[242] Otieno, J. 2014. "Worries over New Avenues of Cybercrime." The East African, September 22. Available ww.theastafrican.co.ke/news/Worries-over-new-avenues-of-cyber-crime/-/2558/2461630/-/vsn7k0z/-/index.html. Accessed 13 June, 2018

[243] Thompson, V. Eric and M'cCants, will (2013) Partner Against Terror: Opportunities and Challenges for U. S. –Moroccan Counterterrorism Cooperation, p.4

[244] Rada, J. 1985. 'Information Technology and the Third World.' In the Information Technology Revolution, Edited by J. Forrester. London: Blackwell.

region.[245]

The cooperation provides an opportunity for evaluation and assessment of own cyber counter threat measures and strategies to discern what has worked and what has not worked. Kenya has traditionally relied on the hard power approach when dealing with cybercriminals as opposed to a hybrid approach. The experience of other countries like US, Europe and South Africa suggest a multi-pronged approach as the most ideal strategy to counter cyber threats.[246] One of the strategies is to first approach cyber threat as an internal security matter that require deployment of early warning system, enforcement agents and legal framework.

In order to enhance the capacity for enforcement, this provides an opportunity for partnership with other nations on cyber security training and intelligence sharing.[247] Kenya requires a relook on its cyber security programmes to incorporate soft power techniques that speak to the root causes of cyber threats within institutions in both public and private sectors. Such techniques include the provision of infrastructure, education and resourcing which can assist the government address any motivation to commit crime through cyber technology.

4.8 Legal Capacity Building

The concept of cybercrime has diverse definitions across the region with every country defining it according to their own perception and needs.[248] This varied definition and considering that every country has its own legal regime, thus cooperation at state level and mutual legal assistance and other

[245] Noor, a.1984. A framework for the creation and management of national computing strategies in developing countries. Computer Journal, Vol.27, no. 3
[246] Heeks, R. strategies for indigenizing IT production in developing countries. Paper presented at the IFIP and Kenya Computer Institute Conference on the Social Implications of Computers in Developing Countries, 23-25 March, Nairobi, Kenya.
[247] Bhatnagar, S.C. and M. Odedra, eds.1992. Social Implications of Computers in Developing Countries. New Delhi: Tata McGraw-Hill.
[248] Ibid. p 45

bilateral arrangements such as arrest of perpetrators are weak.[249] Such weakness is further compounded by limited coordination between law enforcement agencies and judicial officials. All these conspire to impact on the quality of investigation, prosecution and adjudication of cybercrime cases.

The prevailing situation provides an opportunity not only to harmonize legal regimes, but also to develop programs for joint legal experts within the region, judicial officers and law enforcement officials in order to build legal capacity within individual countries and across the region.[250] Such training can be offered by relevant regional, UN ITU agencies or any other partner that may be approached for assistance. The end objective should be to achieve synergy and harmony on cyber security preparedness.

4.9 Partnership with Local Non-State Actors

Ordinarily, Governments have been shy to engage with other players on matters pertaining to security.[251] However, due to the current nature of global insecurity, it is increasingly becoming important that other players such as civil society groups, media and academia are incorporated to discuss options to address issues of cyber threats in order for the state to achieve its national security objectives. This is because some actors have a comparative advantage to reach out to sections of the society that might want to engage in cybercrime activities against the state. Other notable areas where these groups could complement state efforts include; conducting cyber awareness campaigns to sensitize users and promotion of programs aimed at countering the motivations of cybercrime narratives and government efforts to combat the crime.[252]

---

[249] Jackson, T. 2015. "Can Africa Fight Cybercrime and Preserve Human Rights?" BBC News. Available www.bbc.com/news/business-3207948. Accessed 06 May, 2017

[250] Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi and B. Shiyayo. 2014. "Kenya Cybersecurity Report 2014." Available www.seanu.com/downloads/kenyaCyberSecurityReport2014.pdf. Accessed on 20 August 2018

[251] Op.Cit International Council on Human Rights Policy, pp. 49-50

[252] Government of Kenya.2014. Cybersecurity Strategy. Ministry of Information Communications and Technology.

The need to address cyber insecurity while protecting ICT infrastructure thus offers the government real opportunity to establish a framework and platform of cooperation in order to tap into the competencies of these actors. More often than not, the state will react to a situation, only once the damage has been done as the case was for Kenya cybercrime in 2014.[253]

4.10 CHAPTER DATA PRESENTATION, INTERPRETATION AND ANALYSIS

4.10.1 Cyber Security Measures and Strategies to Mitigate Threat

Table 4.2 and Graph 4.1 shows correlations between two quantitative variables of cyber technology and security nexus. The correlation matrix was used to determine the level to which fluctuations in the value of cyber security attributes (dependent variables) was associated with technology (independent variables) Table 4.2 (variable indicators). The data for a correlation analysis consists of two input columns of threats to cyber security. The correlation coefficient (r) is a measure of the strength of the association between the two variables. This coefficient was determined by identifying variables as shown in Table 4.3 below and drawing a scatter plot of the variables to check on the linearity using the Statistical Packages for Social Science (SSPS) programme as shown in Graph 4.1. From analysis the coefficient is supposed to range from -1 to +1: with -1 indicating a perfect negative correlation, +1 indicating a perfect positive correlation, and 0 indicating no correlation at all. When the values are closer to +1 then the variables have a high positive correlation and when values are closer to -1 then the independent variables have a strong negative correlation with the dependent variable. In this analysis the correlation coefficient (r) was normal at a value of 0.80 (r = 0.80) indicating that the correlation is significant at 0.01 level (2-tailed). This indicates that the relationship between the variables is very strong at r = 0.80 or 80% and therefore the data lie on a perfect straight line with

[253] Nzwili, F. 2015. "China and Kenya at odds over Suspected Chinese Cyber Criminals." The Christian Science Monitor, January 26. Available www.csmonitor.com/World/Africa/2015/0126/China-and-Kenya-at-odds-over-sis[ected-Chinese-cyber-criminals. Accessed 10 February, 2018

positive slope as shown in Graph 4.1. The correlation coefficient (r=0.80) shows the strength of association between the two variables and hence cyber technology and security are strongly correlated. The data was then analyzed using 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 = Threat to Security

X_1 = Cyber threats/crimes

X_2 = Cyber patterns

X_3 = Cyber strategies

ε = Erroneous variables

β_0 = Mathematical intercept

Table 4.2: Variables and Indicators for Correlations Inferences

Variables	**Independent Variable (IV)**	**Dependents Variables (DV)**		
	Cyber technology	**Threat to security**	**Cyber patterns**	**Cyber strategies**
Indicators	Software applications	Breaches	Social engineering	Legal Framework
	Social Media	Malware	Denial of service	Awareness training measures
	Internet applications	Hacking	Infiltration	Use of antivirus and pass word

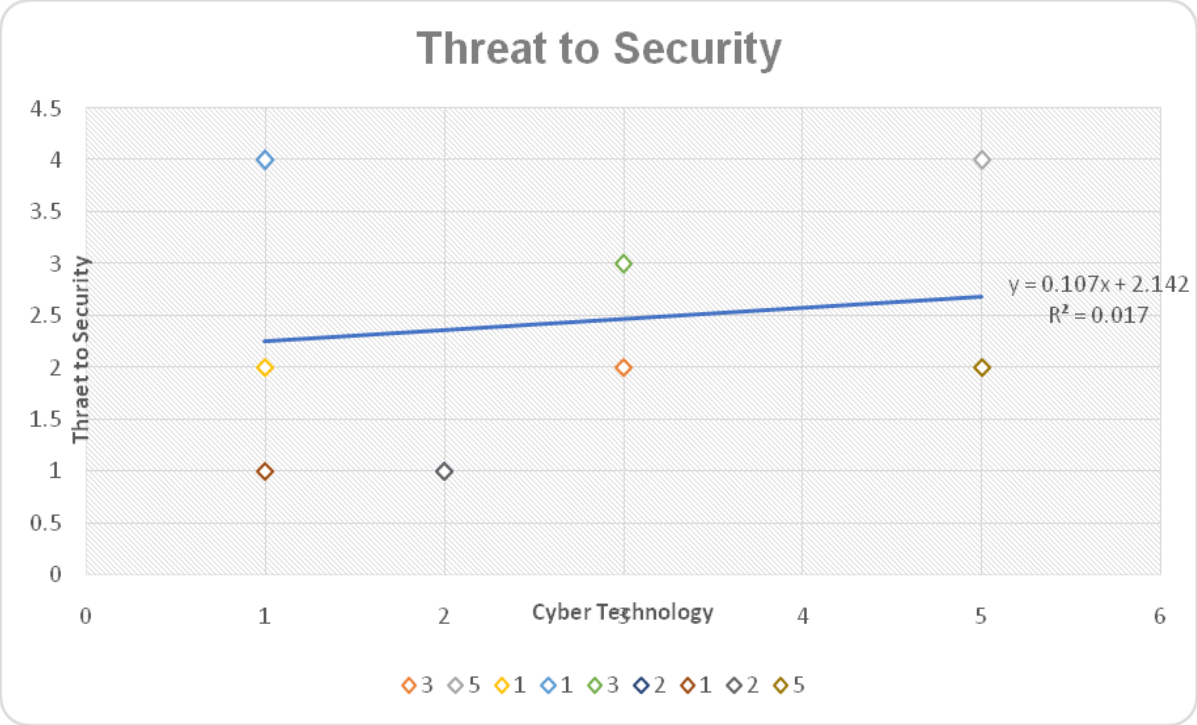
Source: Author (2018)

Table 4.3: Correlations Inferences

		Threat to security	**Cyber Technology**	**Cyber patterns**	**Cyber strategies**
Threat to security	Pearson Correlation	1	.80**	.06	.47
	Sig. (2-tailed)		.000	.539	.719
	N	35	35	35	35
Cyber threats	Pearson Correlation	.80**	1	.426**	.063
	Sig. (2-tailed)	.000		.003	.673
	N	35	35	35	35
Cyber patterns	Pearson Correlation	.06	.426**	1	.213
	Sig. (2-tailed)	.539	.003		.146
	N	35	35	35	35
Cyber strategies	Pearson Correlation	.47	.063	.213	1
	Sig. (2-tailed)	.719	.673	.146	
	N	35	35	35	35
** Correlation is significant at the 0.01 level (2-tailed).					

This research notes that as per the inter-correlation matrix, all the independent variables associate positively with threat to security (the dependent variable) at varying degrees. Similarly, cyber technology and cyber patterns are equally highly correlated with threat to security while cyber strategies are related albeit to a low extent. The cyber strategy showed a very weak correlation with threat to security because this is a counter measure to insecurity that includes cyber threat awareness and the use of antivirus. As shown from the graph the slope tends to learn towards normal line or the gradient tend towards zero which shows the extent of controls or mitigation applied. On the overall, the cyber strategies are measure taken to reduce the effects of attacks. These include policies measures, user awareness straining and use of antivirus. These measures act as catalyst to counter attacks and ensure that it remains at minimum level as shown by the linear association between the variables. The threat is therefore normal with a strength of correlation coefficient of 0.80 which is highly significant than 0.000.

Graph 4.1: Correlation of Cyber Security Measures and Strategies to mitigate threat



Source: Author (2018)

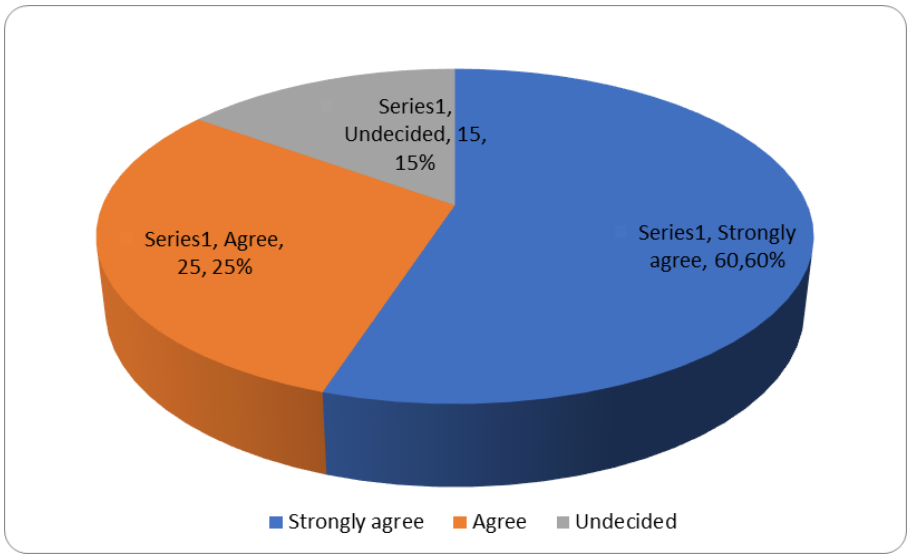
Correlation analysis was done to establish the relationship between the independent variables and the dependent variable. This study proved that there exists a strong positive relationship between cyber technology growth and threat to national security. This correlation is presented by the Pearson Correlation Coefficient of .80** (threat to security), .426** (cyber technology) and .426** (cyber patterns) while there was no weak positive relationship with cyber strategies or cyber defence, Table 4.3. This clearly points at a need to invest more on cyber awareness training and antivirus software as a means of defence to avoid attacks. This corroborates with the efforts and strategies that have been put in place in Chapter 4.2 to 4.4 above.

4.10.2 Counter cyber security measures and strategies applied in Kenya

This study sought to know if respondents were cognisant of the existence of cyber security policies, laws and regulations and whether there exist any gaps. 60% strongly agreed that Kenya has cyber security measures and strategies to address cyber threats, 25% Agreed and 15% were unaware as shown in Pie Chart 5.1. The data collected through the literature review and the interview with the respondents shows that there is lack of awareness on information security matters in most of the organizations.

This study observes that whilst the policies on cyber security exist enforcement is weak and therefore exposes the institution to attacks. On identifying specific cyber laws, the same respondents were asked to identify the policies and laws they knew; 60% were able to list them, 30% had difficulty to remember them all while 10% were not able. This observation links quite pertinent in that the government has taken cognisance and has developed national cybercrime management framework. This framework consists of ICT policies and legislations, yet cyber security continues to be a problem. This linkage is therefore essential when considering that the role of organizations and how they have invested in their own security especially on sensitive intuitions like security departments, banks and IT. When asked to suggest possible solutions, 65% respondents agreed that there was need to develop a specialised information security courses in schools and colleges while 35% insisted that the institutions should create awareness programmes. In addition, all respondents agreed that institutions must develop regulations with respect to enhancing cyber security awareness in their work place. These sentiments correlate with the literature in Chapter 3 paragraph 4.1. In this way, the findings confirm the gaps identified in the literature and hence the rationality of the research.

Pie chart 4.1: Counter cyber security measures and strategies



Source: Author (2018)

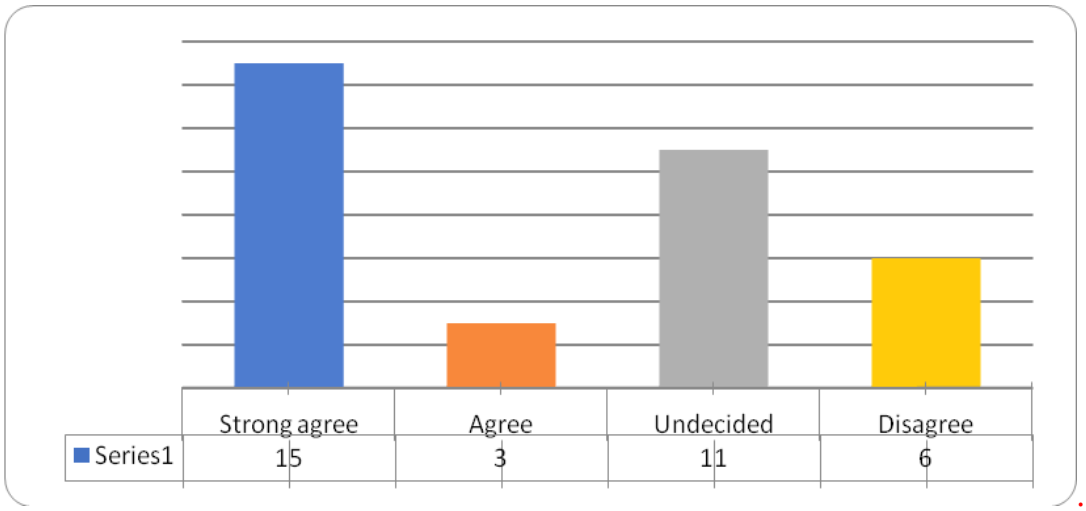
4.10.3 Knowledge on cyber security laws in Kenya

This study was conducted to confirm if respondents had information on the existing cyber security policy, legislation and regulations to protect the ICT infrastructure. The respondents were asked to name some of these laws and frameworks. The findings and frequency of response is as shown in Pie Chart 3.2. Most of the respondents agreed that Kenya has existing policies, laws and regulations on cyber security. Majority of them were able to name them as shown in Table 3.4. Whereas, most of the respondents were able to name most of the legal framework however, they were not very familiar with the "Kenya National Cyber Security Master Plan 2017/2018" and its contents. When asked whether there were any other strategies that the Kenya has put to address cyber security issues, a few were able to name and state the purpose of the Kenya Computer Incidence Response Team Coordinating Centre as an advisory body on cyber security matters.

4.10.4 Achievements in the fight against cyber threats

The respondents were asked to state if Kenya has achieved in the fighting cyber threats. The outcome showed that 15% strongly agree, 3% agreed, 11% undecided while 6% disagreed as shown in Bar Chart 4.2. From this analysis, the understanding on whether there are any achievements in the fighting security efforts was scanty. The 15% and 3% of the respondents who agreed observed that while the country has policies, legislation and regulations in place, cybercrime is on increase. When asked whether they report cases of attacks to the police, 15% agreed but noted that there were no efforts to pursue the attackers. When asked what the cause of the problem was, 15% blamed on the gaps in the existing cyber security laws, lack of awareness, lack of capacity on the security experts and lack of support from the organization management. Similarly, the respondents were asked to name the institutions most affected by cybercriminals. 70% named banks and financial institutions, government offices, security organizations, legal institutions and IT institutions. When asked what motivates the criminals, 80% indicated financial gains, obtain information, malice and fantasy.

Bar chart 4.2: Achievements in the fight against cyber threats



Source: Author (2018)

This finding agreed with the literature review in Chapter two section 2.7 observed that Kenya lacks basic awareness as an element of national cyber security effort to combat cyber threats. This assertion agrees with findings in (Pie chart 2), and clearly show existing gaps in the legislations and awareness. This can further be argued that the vulnerabilities were high because of lack of corresponding defence capabilities. These sentiments agree with the literature review in Chapter 3 paragraph 3.5.1 which confirms the same argument. The (Pie chart 6 and 7 and Bar chart 1) corroborated with the report contained in Chapter 4 paragraph 4.4.1. These finding are also linked to literature in Chapter 2 section 2.2 which concur with the observations.

4.11 Summary of the Chapter

This chapter notes that by embracing the securitization theory framework, hypothesizes cyber security as a discrete sector with unknown set of referent objects on threats. It is believed that networked security is an important referent objects of the state security with political significance which emanates from links to the combined referent objects that arise from society and the economy of the state. Cyber insecurity with its complexity has demonstrated that it is not easy to combat due to its character and the economics that fevour criminal.[254]

In summary, the chapter presented descriptive data and inferential analysis that was also set in charts, tables and graphs for explanation. The professionals interviewed from ICT sector were also considered to verify the data that were obtained through the internet and libraries. These were analysed in detail to draw interpretations as to the meaning of the data in terms of the study objectives. This chapter agrees that there is lack of consistency amongst the law enforcement and judiciary hence complicating prosecution of cyber cases. Similarly, owing to lack of training and awareness on the cyber

[254] Quarshie, H. O. and A. Martin-Odoom. 2012. "Fighting Cybercrime in Africa. "Computer Science and Engineering 2(6):98-100.

security policies, legislative frameworks and regulations, the fight against cyber threats will remain a challenge until a consensus is established. The next chapter presents the summary, conclusions and recommendations of the study.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter summarises the whole study. The objectives of the study are again stated as well as the methodology used. The data presented, interpreted and analysed guides the researcher to make value judgement on the challenges that the region faces in providing for energy and the collective solutions being pursued. The summary makes key conclusions and important recommendations on the way forward.

5.2 Summary of the Study

This study intended to explore the connection between cyber technology and insecurity in Africa using the case of Kenya. The study was prompted by a growing cyber threat to Kenya's national security yet there are measures that have been developed to protect the ICT infrastructure. The study sought to to understand why cyber security continues to be a problem, what are driving them and what can be done to improve the situational awareness of Kenya.

In order to enhance understanding of the problems under study, literature was reviewed eagerly following the research objectives that the study sought to achieve. The literature identified gaps existing in the ICT sector. The main objective of the study is to establish cyber technology and in-security nexus in Africa using a case study of Kenya. The specific objectives of the study included: To examine the cyber technology security nexus in Africa. To assess the emergent patterns of cyber technology as a national security threat in Kenya and to evaluate cyber security measures and strategies applied in Kenya.

In order to obtain answers to the objectives of the study, the researcher used both qualitative and quantitative methodologies. The study considered the efforts made by Kenya to address cyber security threats. The study targeted respondents who included ICT professional from various government ministries, security sector, diplomatic officials, academia, IT institutions and other sectors. The data was collected through the internet, libraries and the interviews which targeted ICT professionals.

5.3 Summary of the Findings

The literature presented in Chapter 3 and 4 indicate that Kenya has embraced e-economy as a national development priority and has further created security policies and legal framework to address the challenges facing the business infrastructure now and in future. This study concurred that there are various security measures that can be applied to protect ICT industry against cyber-attacks. However, the research notes that while Kenya has developed cyber security measures and strategies that include legal framework, they have not been able to address cyber security threats appropriately.

This study took note that most Kenyans remained vulnerable to attacks because of lack institutional security measures. The research found out that there was gross lack of cyber threat awareness amongst many internet users. This level of ignorance allows the criminals to continuously attack without any form of alertness to facilitate mitigation. It is through this absence of situational awareness that the government and financial institutions have lost huge sums of funds or valuable information. This shows that these efforts are not appropriate enough to decisively achieve cyber security. Clearly, the strategies points at national weaknesses to monitor, detect and prosecute offenders as necessary. The cyber security measures that are in place are therefore not adequate to address the current security issues. This is because most organizations do not have established security practices needed to protect critical cyber infrastructure. In view of this Kenya, needs to review the current

measures with a view to developing strong and clearly defined national cyber security strategies that encourage threat management practices which can anticipate, detect, respond and contain cyber security threats.

Concerning the research methodology, the study made use of a mixed methodology that incorporated the quantitative and qualitative approaches adopted in the survey research design. A total of 50 structured questionnaires were self-administered to ICT professionals from various sectors and structured interviews were conducted. Although the study faced the risk of low response rate due to sensitivity of the study, the overall outcome of the study revealed that most of the staff remained grossly unaware of the various cyber-attacks which threaten their institutions and subsequently national security. This meant that there was a strong relationship between cyber technology and in-security. The results of the study were also validated by the fact that most of the respondents have long and varied experiences in respect to the ICT sector. The research showed that the average ages of the managers were between 30 - 39 and 40 - 50 years which indicate their level of experience. This was important in validating the research findings.

5.4 Conclusions

Basing on the objectives of the study and in view of the above findings, the following conclusions are drawn that there is a relationship between cyber technology and in-security. The study concluded that these were a strong relationship of correlation between the growth in technology and in-security. The increased advancement in technology has led to increased cybercrime. The research found out that there was gross lack of cyber threat awareness amongst many internet users. This level of ignorance allows the criminals to continuously attack without any form of alertness to facilitate mitigation. There was lack of institutional involvement in cyber security issues. The increasing recognition of the important role

played by institutions through investing in cyber security is a major step towards enhancing cyber threat capacity.

5.5 Recommendations

This scholarship on the relationship between cyber technology and in-security has brought to light realities and gaps that are inherent in the overall strategy of cyber security. Some of the realities are often assumed, which in the overall impacts on the effectiveness of cyber security measures and strategies. In certain instances, the nature of the environment under which cyber security agents operate is not a normal one. Sometimes, accusations are directed at security agents without proper appreciation by the accusers of the background details. The cure for this gap can only be addressed by policy. This research recommends that there is need for cyber policy to sensitize general Internet and ICT users on the risks they are exposed.

5.5.1 Policy Recommendations

The interest of Kenya to embrace cyber technology as a platform of economic development and the need to protect the nation from cyber threats do not conflict. The two are aimed at securing the nation where individuals and organizations are free to pursue their aspiration in an environment that is peaceful and secure. The point of divergence is in the approach and mechanics of achieving this. Noting that cyber security is a global responsibility and there is need for collaboration with stakeholders from the region and globally to enhance the capacity in managing cyber threats. Moreover, the need to sensitize employees on cyber security potential threats is a critical aspect of policy that should be in place.

The policy should also be expanded to include multi-agency counter cyber measures and strategies that incorporates international best practices organizations and other stakeholders. The focus

on such measures should be long-term and geared towards enhancing cyber security awareness. The national approach towards cyber security should mainstream the use of intelligence to drive operations. A robust policy with an effective monitoring and evaluation mechanism be put in place to determine the relationship between the cyber threats and cyber security measures and strategies adopted. The policy to have activities and programs that bring the two elements together in order to minimize the embedded suspicion and mistrust.

The capacity gap noted within the ranks of security agencies need to be addressed through training. For effectiveness, such training should be conducted within a multi-agency setting such as KE-CERT. It should hence incorporate elements from the judiciary, security agents such as the cyber police units, KDF, media and individual cyber café operators.

Cyber awareness is the most effective weapon on matters that touch on cyber protection strategies on basic security related issues that are critical for the security of the nation. It is recommended for the government to make a deliberate effort in awareness creation and to promote patriotism among the youth. This can be done through school-based e-learning programs. Occasionally, the media can also be used as a channel to create awareness. Knowing their responsibilities the internet technology users will help enjoy the services while at the same time help to protect the nation from cyber threats.

This study highly recommends the developing cyber risk management frameworks, to enable clients to assess their compliance with laws, regulation and best practice relating to cyber risk that is preparing for cyber breaches, including designing tailored cyber response plans.

5.5.2 Benefits of the Study

The study has brought out challenges of cyber technology and security threats that Kenya has to contend with, on daily basis in their quest to ensure safety in the infrastructure. It has also exposed various weaknesses that are inherent in the whole cyber security measures and strategies. The information provided can be used as a base to formulate policies that can help to promote safe cyber usage while at the same time enhancing national cyber security. There is need to involve academia in research and development (R&D) including innovation to develop appropriate computer protection that is easy to use and less costly.

5.5.3 Suggested areas of further studies

The study has been on general outlook of cyber technology and in-security challenges facing Kenya and in essence Africa. The findings are presented with common adage of asymmetric cyber threats to national security. The threat seems to defy existing strategies and measures put in place. It was noted that there is a general lack of empirical studies on cyber technology and implications on security. This situation has led to loses of government information while financial institutions continue to report loses of funds. In the circumstance, there is need to research on home grown solutions based on the local environment. These are areas that have been left out and may require further investigation to determine how they play out in the broad context of cyber technology and in-security.

BIBLIOGRAPHY

Abraham, D. The Best Defense? Legitimacy and Preventive Force, Stanford, CA: Hoover Institution Press, (2010).

African Development Bank Group, Africa is now the fastest Growing continent in the world", 7 November, (2013).

African News. (2010b), Kenya: Banks Fight to Secure Customers Deposits from Cyber Criminals. Business Daily (Nairobi, 2010).

African Union Commission and United Nations, Economic Commission for African, Making the Most of Africa's Commodities: Industrializing for Growth, Jobs and Economic Transformation: Economic Report of African 2013, (United Nations Publication), Sales No: E. IIK.1., (2013).

African Union, Draft Convention on the Establishment of a Legal Framework Conductive to Cyber security in Africa. Common Market for Eastern and Southern Africa (COMESA), Cyber security Draft Mode Bill, (2012).

Akamai, The State of the Internet, Q1 FY (2017).

Akogwu, S. An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria (Unpublished B. Sc project). Department of Sociology, Ahmadu Bello University, Zaria, (2012).

Akubue, A Appropriate Technology for Socioeconomic Development in Third World Countries. The Journal of Technology Studies 26 (2000).

Alexis, O. SMSs used as a tool of hate in Kenya, (2016).

Alsmadi, I. Security Challenges for Expanding E-government' Services. International Journal of Advanced Science and Technology, (2011).

Arbor, F. Networks. Worldwide infrastructure security report, (2006), p.77

Aronson, S.L. Kenya and the Global War on Terror: Neglecting History and Geopolitics in Approaches to Counterterrorism. African Journal of Criminology and Justice Studies: AJCJS, Vol 7, (2014).

Asia Pacific Computer Emergency Response Team. The Cyber Green Initiative improving health through measurement and mitigation', Concept Paper (Japan Computer Emergency Response Team Coordination Centre, 2012).

Aus CERT 2006. Computer crime and security survey.
Hip://www.auscert.org.au/images/ACCSS2006.pdf.

Balancingact.africa.com, Impact of Cyber Fraud on Kenyan Banking Sector, Devastating. (2010)

Bandara, I. Iroras, K. Maher, C. Lusuardi – CYBER SECURITY CHALLENGES OF DISTRIBUTED E-LEARNING SYSTEMS, (2015).

Bank Supervision Report. Annual Report, Central Bank of Kenya, (2013).

Baumartner, F.R. and Jones, B.d. Agenda and Instability in America Politics. Chicago: University of Chicogo Press, (1993).

Beate Stollberg, Tom de Groeve, The Use of Social Media within the Global Disaster Alert and Coordination System (GDACS), WWW-SWDM'12 Workshop April 16-20, 2012, Lyon, France, (2012).

Biztech Africa (2011, October 29). Safaricom unveils cloud deployment. Available in http://www/biztechafrica.com/section/internat/article/safaricom-unveils-largestnative cloud-deployment-/1365/.Accessed 03 January, 2018.

Borg, R and Gall, D. Education Research. 6th Edition. New York Longman Inc (1996).
Brauch, P, I, et al. (eds), Coping with Global Environmental Change, Disasters and Security, Hexagon Series on Human and Environmental Security and Peace 5, DOI 10.1007/978-3 642-17776-7_2, © Springer-Verlag Berlin Heidelberg, (2011).

Brenner, S. Law in an Era of Smart Technology, Oxford: Oxford University Press, (2007).

Brenner, W Cybercrime: Criminal Threats from Cyber Space. Santa Barbara, California: Greenwood Publishing Group, (2010).

Burt, D., Nicholas, K.S., Scoles, T. The cybersecurity risk paradox: impact of social, economic, and technological factors on rates of malware, Microsoft Security Intelligence Report Special Edition (SIR), MIscroft Corporation, (2014).
Carrier, N and Lochery, E. Missing States? Somali Trade Networks and the Eastleigh Transformation. Journal of Eastern African Studies 7 (2013).

Central Bank of Kenya Governor Patrick Njoroge during the Monetary Policy Meeting in Nairobi held amid backdrop of improved weather conditions on May 30, (2017).

Central Bank of Kenya GUIDANCE NOTE ON CYBERSECURITY, (2017).

Central Bank of Kenya, December 2008 Survey on Bank Charges and Lending Rates http://www.centralbank.go.ke/downloads/bsd/Survey2009.pdf

Chava, F. and Nachmias, D. Research Methods in Social Sciences. London, (1985).

Chavan, G. R., Rathod, M.L., &Naik, N. (2010). Cyber Crime:A study. SRELS Journal of Chetty I and Basson A. Report on internet usage and the exposure of pornography to learners in South African schools. Research report for the Film and Publication Board, Houghton, South Africa, (2006).

Clark, K., Stikvoort, D., Stofbergen, E., & van den Heuvel, E. A Dutch Approach to Cybersecurity through Participation. Security & Privacy, IEEE, 12(2014), 27-34.

Cohen, L and felson, M. Social change and crime rate trends: A routine activity approach, Americac Sociological Review, (1997).

Collins, A. Contemporary Security Studies, (UK: OUP,2013).

Colwill, C. and Gray, A. Creating an effective security risk model for outsourcing decisions. BT technology journal 25(2007).

Communication Authority of Kenya, (2016).

Constitutional implementation in Kenya, 2010-2015: challenges and prospects, FES Kenya Occasional Paper, No.5 ISBN: 9966-957-20-0.

DAILY Nation (2010) Kenya: Alarm as bank employee siphon out Sh2.4bn through "inside JOBS" 10TH July 2010 Available at http://allafrica.com/stories/20100712388.html (Accessed on January, 218).

Daily nation August 3, (2016).

Daily Nation. 2015. Try Crime Suspects Here. Daily Nation, January 15. www.nation.co.ke/oped/Editiorial/ChinaKenya-Hacking-Trial/-/440804/2590722/fcv6rlz/-/ index.html.

David, W. Cybercrime, the Transformation of Crime in the Information Age, Polity, (2007).

Dhiraj, M. and Scott A. Longwell, Twitter and Disasters: The uses of Twitter during the 2010 Pakistan floods, (May 2012).

D'Ovidio, R and Doyle J. A Study on Cyberstalking: Understanding Investigative Hurdles, FBI law enforcement bulletin, (2003).

Draft Meeting report: ITU Regional Cyber Security Forum for African and Arab States held in Tunisia, Tunisia (2009).

Duncan, B, H. and David, G.P. Do Cyber-Attack Require a Duty to Assist? Law Technology News, (2010).

ENISA, "ENISA threat Landscape 2013 – Overview of Current and Emergency Cyber Threats," 2013, available at www.enisa.europa.eu/activities/risk-management/evlvingthreat environment/enisa

Threat-ladscape/enisa-threat-landscape-2013-overbiew-of-currentand emergency-cyber- threat/at download/fullReport.

Eric,T.The AU's Cybercrime Response, ISS Policy Brief 73, (January 2018).

Evans D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything'. Cisco white paper Cisco Internet Business Solutions Group, (2011).

Fischer, E. Creating a National Framework for Cyber security: An Analysis of Issue and Options, February 22, CRS Report for Congress, Order Code RL32777, (2005).

Foreword, Kenya Information and Communications (Amendment) Act, (2013).
Friman, H.R. Crime and Globalization. In H Richard Frima's(ed) Cyber and the Global Political Economy. International Political economy, Yearbook, Boulder.Lynne.Rlemer Publishers, (2009).

Gady, F.S. Africa Cyber. Foreignopolicy.com/articles/2010/03/Africa cyber.wmd. (2010).

Gagliardone, I., and Sambuli, N. Cyber Security and Cyber Resilience in East Africa. Centre for International Governance Innovation, (2015).

Gercke M. The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International, (2006). Gergle, M. understanding cybercrime a guide for developing countries; Geneva International Telecommunication Union, (2011).

Gesser, U., Maclay, C, and Palfrey, J Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations, an Exploratory Study by Barkman Center for Internet and Society at Harvard University in collaboration with UNICEF.
Http//www.cyberdigital safety.developing.nations,(2010).

Global Cybersecurity Index (GCI, 2017).

Government of Kenya, Government of Kenya Vision 2030, (2007).

Goldman, S. eCommerce expected to accelerate globally in 2014, Equity Research, New York: The Goldman Sachs Group, Inc.,5 March (2013).

Gordon S. and Ford, R. Cyberterrorism? In: Cyberterrorism, The International Library of Essays in Terrorism, (2014).

Government of Kenya. Cybersecurity Strategy. Ministry of Information Communication and Technology, (2014).

Hassan, A.B., Funmi, D.L., and Makinde, J Cybercrime in Nigeria: Causes, Effects and the Way out. RPN Journal of Science and Technology, 2(2012).

Hold Security. You have Ben Hacked! Internet//http//www.holdsecurity.com/news/cybervor breach, (2012). Holloway, P. and Galvin, L. (2016).

Holt, T.J. Sub-cultural evolution. Examining the influence of on and off-line experiences on deviant subculture. Deviant behavior, 28. (2007)

Ibrahim, M. Somalia and Global Terrorism: A Growing Connection? Journal of Contemporary African studies, Volume 28:3, (2010).

ICT Authority, "Kenya's ICT Master Plan 2014-2017;" ICT Authority and C4DLab, "Cybersecurity Training'" 2014, available at http:www.c4dlab.ac.ke/training/cybersecurity.

ICT Authority, Kenya, the Kenya Cyber Plan 2013-2017, (2016).

International Telecommunications Union, "ICTs facts and figures 2015"' ITU Telecommunication Development Bureau (Geneva, 2008)

International Telecommunication Union. "ICTs facts and figures 2013". ITU Telecommunication Development Bureau (Geneve, 2008). Available from www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

Internet World stat, (2017).

ITU (2014) 'World Telecommunication.ICT Indicators database', 18th edition. Available at: http://www.itu.int/en/ITUD/Statistics/pages/publication/wtid.aspx

ITU, "The World in 2016 ICT Facts and Figures" http://www.itu.int/en/ITU-D/Statistics/ Documents/facts/ICTFactsFigures2014-e.pdf,2015-04-17. Accessed on 02 Jan 18

ITU, "UNDERSTADING Cybercrime: A guide for developing countries;" Symantec, "Internet Security Threat Report;" Kaspersky, "The Threat landscape;" F-Secure lab, "Mobile

Threat Report," 2013, available at www.f-secure.com/static/doc/labs_global/Research/ Mobile_Threat_Report_Q3_2013.pdf; McAfee, "McAfee Lab Threat Report: Third Quarter2013," 2013, available at http://www.mcafee.com/uk/resources/reports/rp quarterly-threatq3-2013.pdf.Accessed on 08 February, 2018.

ITU, "Understanding Cybercrime: A guide for developing countries", Symantec, "Internet Security Threat Report'" 2014 available at http://www.symantec.com/content/en/us/ Enterprise/other_resources/b-istr_maim_report_v19_21291018.en-uspdf;Kaspersky, "The Threat landscape," 2014, available at http://media.kaspersky.com/en/business security/kaspersky-threat-landscape-it-online-security-guide.pdf.

ITU. 2015. ICT Statistics. AVAILABLE www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspsx.

John. O. S. Growth and other good things, The Economist, (2013).

Juma V. Online Shopping Kenya Consumers Out of KRA Reach, (2010) l Http//www.businessdailyafrica.com.

Justine, O. S. Growth and other good things, The Economist, (1 May 2013).

Kagwanja, P., and Karanja, M. (2014, AUGUST 18). How cyber-crime complicates war on terror. The East African, Retrieved from http://www.theeastafrican.co.ke/news/How cyber-crime-complicates-war-on-terror/2558-2422854-13ja90iz/index.html

Kamau, M (2011), Policy site Defacing Shows Cyber Crime is Rising. Http//www. Stanardmedia.co.ke/insightpage.200006361. Accessed 08 December, 2017

Kimini, D. Cyber Crime in the Society: Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences, (2011).

Kearney, M., Schuck, S., Burden, K., and Aubusson, P. Viewing mobile learning from a pedagogical perspective, Research in Learning Technology, (2012).

Kedmey, D., Wold Global health. United Nations Population Fund. New York, United States of America, Vol. 6, (2014).

Kelly, T., Minger, M. and Yamanishi, E. Information and Communication for Development, Maximizing Mobile. The World Bank, (2012).

Kemibaro, M. (2011, October). Safaricom CLOUD: Safaricom's third act to dominate Kenya's Telecoms sector? http://www.moseskemibaro.com/2011/10/29 safaricomcloud safaricoms-thirdact-to-dominate-kenys-telecoms-sector/. Accessed 05 January, 2018

Kenya Cyber Security Report, (2016), p 4.

Kenya Cybersecurity report, 92015).

Kenya Gazette Supplement, ACTS, (2013).

Kenya Vision 2010 of October, (2007).

Kenya's Computer and Cybercrimes Bill, (2016).

Kenya's Cybersecurity Framework and Realate Draft KICA REGULATIONS, (2016)

Kenyan National Commission on Human Rights (2008) Idid. Para 71, p29. See also Kriegler Commission (2008).

Kigen, et al, 2014. "Kenya Cybersecurity Report 2014." www.serianu.com/downloads/ KenyaCyberSecurityReport2014.pdf

Kigen, P. M., Muchai C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., and Shitanda, S. Kenya Cyber Security Report 2015. Serianu Limited, (2015).

Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M Mwangi and B. Shiyayo. 2014, "Kenya Cyber Security Report 2014." www.serianu.com

Kinyanjui, K. Watchdog Warns of Increasing Cybercrime Threat. (2006).

Kornakor, K. (2006). Police Forces in East Africa will have a New Hi-tech Lab.Http//www.viruslist/news.197753850. Accessed on 08 December, 2017

KRA. (2011). KRA Online Services. http://www.kra.go.ke/index.php/kra-portal.

Lawrence, G. Cyber Threat Trends and U.S. Network Security, Statement for the Record to the Joint Economic Committee, National Intelligence Council, (2001)

Lewis, A.J. Assessing the risks of Cyber Terrorism, Cyber War and Cyber Threats, Journal of Centre for Strategic and International Studies, Washington DC, (2002).

Liebowitz, M. Cyber gang stle $5 Million in 72 hours, (2018), pp. 27-31.

Longe O. B, and Chiemeke S. C. Cybercrime and Criminality in Nigeria – what roles are internet access points in playing? Eur. J. Soc. Sci. 6(2008), pp. 133-139.

MacAfee 2014, MacAfee Labs Threats Reports.

MacAfee 2014, MacAfee labs Threats Reports. Internethttp//www.macfee.com/hk/resources//reports/rp-quarterly-threats-q1-2015.pdf

Macharia Kamau, "Kenya wants EAC States to hasten Fake Phone Switch off." Standard Digital, 28 June 2013, http://www.standardmedia.co.ke/business/article/2000086969/kenyawants-eac-states-to hasten-fake-phone-switch-off 7/07/2013; winfred Kigwe, "Kenya: 1.9 million Fake Phones Shut," All Africa, 2 October 2012, available at http://allafrica.com/stories/201210020512.html. Accessed on 06 February, (2018).

Maina, E A survey on impact of ICT on Business Value Creation in Kenya Ban King Sector. Unpublished MBA project, University of Nairobi, (2010).

Maliti T. (2010). New cables to Tie Africa ti Internet, http//www/washingtontimes/news/2010/sep/1/new-cables-to-africato-internet. Accessed on 13 December, (2017).

Maliti, T. New Cables to tie Africa to internet, (2010).

Mallory, S. L. Understanding Organized Crime, Jones and Bartlett, (2007).

Mark. P. Intelligence theory and theories of international relations: shared worlds or separate ? In intelligence Theory: Key questions and debates. Studies in Intelligence,

(London: Routledge, 2009).

Marwick, A and Boyd, D. The Drama! Teen conflict, gossip, and bullying in networked publics. Draft version of paper to be submitted at the oxford Internet Institute's 'A decade in internet time' symposium on the dynamics of the internet and society, (2011)

Mantinde, V. high Data Cost and factors of Mobile Insecurity in Africa. IDG Connect, (2014).

Mauritius ICT Indicator Portal. International indice. Maurious National Computer board, (2011).

McPhie, E. Building capacity to narrow the digital divide in Africa from within. World Economic Forum-NEPAD E-ReadinessPolicy Programme, (2003), p. 18.

Mengo, B. Urban Cyber Space Under Criminal Siege, (2011).

Mike, O. Africa poised for unprecedented, lont-term economic growth: Seven drivers that could Transform Africa into the world's economic powerhouse, International Business Times, (2013).

Misiko H (2014, July30). How Anonymous and other Hackitivists are waging war on Kenya. The Washington post. Retrieved from http://washingtonpost.com/news/worldviews/wp/. Accessed 20 February, 2018.

Moeng, B. Reasons to invest in Africa ICT. IT News Africa, (2017).

Muhumuza, M (2010), East Africa EAC Prone to Cyber Crime, say experts Http//www.allafrica.com/stories/201008240531. Accessed 09 December, 2017.

Matua, W. The Significance of Mobile We in Africa and in future. (2011).

Muwanga, D. (2011), East Africa Asked to Build Cyber Science School. Http//www.busiweek.com. /11/opportunities/1997/east Africa science school. Accessed 6 December, 2017

Mwenesi, s. 2014a. "ICT Contribution to Kenya's GDP now at 12.1%" Human IPO, July 22. www.humanipo.com/news/46203/ict-contribution-to-kenyan-godpnow-at-12-1. Accessed 10 February, 2018.

Norman, K., Denzin, Y and Yvonna, L. The SAGE Handbook of Qualitative Research, (2000).

Norton Cyber-Crime Report, (2016).

Otieno, J. 2014. "Worries over New Avenues of Cybercrime." The east African, September 22. www.theastafrican.co.ke . Accessed on 20 January, 2018.

Otuki, N. 2014. "Beijing Says Runda Fraud Ring Likely Targeted China, "Business Daily,

December 5. www.businessdailyafrica.com/Beijing-say-Rundafraud-ring-targeted China/-/539546/2546306/-/item/0/-/v9hr5bz/-/index.html. Accessed 11 February, 2018.

Paul. D. Leedy, practical Research. New Jersey: Prentice-Hell, (1997).

Paula, K., Carol, M., Kevin, K., Martin, M., & Barbara, S. Kenya Cyber Security Report. Nairobi, (2014).

Pawlak, P. Developing capacities in cyberspace', in Pawla, P. (ed) Riding the digital wave: The impact of cyber capacity building on human development, ISSUE, report nr 21, (2014).

Ranz-Stefan, G. Foreign policy: Africa's Internet threat, National Public Radio, 92010), p. 29.

Reilly, M. Beware, Botnets, Have You PC in Their Sights, New Scientist, Vol 196, (2007).

Report on Africa 2013, (United Nations Publication), Sales No.: E.13.IIK.1. p.6. Accessed on 04 November, 2017

Report on Africa 2013, (United Nations publication), Sales no.: E.13.IIK.1., p.6.

Romero-Mariona, J., Ziv, H., Richardson, D. J., & Bystritsky, D. Towards usable cyber security Requirements. In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies. (2009).

Schell, B. H. and Clements, M. "Cybercrime: A Reference Handbook," ABCCLIO, (2004).

Section 3, Draft Cybercrime Bill of Kenya (2014).

See Dana Sanchez, "Without Laws governing Cyber Crime, Is Africa Safe for Cyber Criminals?", February 16, 2015. http://afkinsider.com/88623/without-law-governing cyber-crime-africa-safe-cybercriminals, 2015-06-02; also see Judith M C. Tembo, "Workshop on Tanzania National Transposition of SADC Model Law", 4th-5th February, 2013, http://afkinsider.com/88623/without-law-governingcyber-crime-africa safe-cyber-criminals,2015-04-19.

See, e.g., Hackers Deface Army's Web Site, APBNEWS.COM, (June 28, 1999), at http://www.apbnews.com/newscenter/breakingnews/1999/06/28/hack0628_01.html. Accessed 10 February, 2018.

See,e.g., Seminar on the role of Internet with regard to the Provision of the International Convention on the Elimination of All forms of Racial Discrimination, Item V (Prohibition of Racist Propaganda on the internet Juridicial Aspects, International Measures), U.N. HIGH COMMISSIONER FOR HUMAN RIGHTS, (Nov. 10-14, 1979), at http://www.unhchr.ch/html/menu2/10/c/racism/shahi.htm: Accessed 10 February, (2018).

See, wwe. Opendata.go.ke Open Data Network www.opendataresearch and Majee (20120 and Rahemtulla, et at (2011). Accessed 05 February 2018.

Seniaru, (2016).

Serianu consultants in Cyber Security (2015); available at Ahttp://www.usiu.ac.ke/oncampus/news/296-serianu-usiu-africa-pkf-consulting-launch Kenya-cybersecurity-report-2015.

Serianu, "Kenya Cyber Security Report, (2012).

Serianu, Kenya Cyber Security Report, (2014).

Sheptycki, J., Policing, intelligence theory and the new human security paradigm: some lessons from the field, in intelligence Theory: Key Questions and debates. Studies in intelligence, (London: routledge, 2009).

Shinder, E. 2Ed Scene of the Cybercrime: ISBN: 978-1-59749-276-8, (2002), p.89.

Siegel, J. A., Saukko, P. J. and Knupfer, G C. Encyclopedia of forensic Sciences, Academic Press, (2000), p. 67

Steele, Robert d. "Hackers and Crackers: Using and Abusing the Networks. "Presentation at the fourth Annual Conference on computers, Freedom and Privacy, Chicago, (1994), p. 70.

Symantec Corporation, (2012).

Symantec Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18. Available from www.symantec.com/content/en/us/enterprise/other_resources/b Istr_main_report_v18_2012_21291018.en-us.pdf. Accessed on January, 2018.

Symantec Corporation, Internet Security Threat Report2013, 2012 Trends, Volume18. (2013).

Symantec Corporation, Norton Cybercrime Report, (2012).

Symantec, "Internet Security Threat Report;" Serianu Ltd., "Kenya Cyber Security Report," 2012, available at www.serianu.com/doenloads/KenyaCyberSecuriryReport2012.pdf.
Technology Banker. (2012). Fraud solutions for Africa Banks: A Kenya perspective. Available at http://www.technologybanker.com/security-risk-management/fraud-solutions-for africa-banks-a-kenyan-perspective#.VEKp3fldXg9. [Accessed on 15 January, 2018]

The Commission of Inquiry on Post-election violence (known as the Waki Commission after the Chairman of the Commission Justice Philip Waki) investigated the reasons for the violence and released its findings in a report known as the Waki report. The Independent Review Commission (commonly known as the Kriegler Commission after the Chairman Judge Johann Kriegler) investigated the Kenyan electoral system. The Kenya National Commission for Human rights (KNCHR) released their report, on the Brink of a Precipice, based on investigations and victim's testimonies. See Waki Commission (2008)

Ibid. Kenyan National Commission on Human Rights (2008) on the Brink of the Precipice: a Human rights Account of Kenya's Post 2007 election violence: www.knchr.org/Portals/0/Reports/KNCHR|_REPORT_ON_THE_BRINK_OF_THE_PECIPE.pdf

The East Africa, Kenya Launches Centre to fight cybercrime, (2016).

Tom, J. Can Africa Fight Cybercrime and Preserve Human Rights? (2015).

United Nations Department of Economic and social Affairs (2011) 'Cybersecurity: A global issue demanding a global approach' (New York, UNDESA, 2011) Available at: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global approach.html [Accessed: 03 January, 2018]

UNODC Comprehensive Study on Cybercrime, (2013).

UNODC, World Drug Report 2013 (United Nations publication, Sales No.E.13.XI.6).

Wankiku, r. (2011), Rising Cybercrime Pushes Africa Government to Take Action. Computer world Kenya. Http//www.news.idg.id6EF9B560-ODDE-E2CB-4D0981F70155CC24. Accessed on 05 December, (2017).

Wanjiku R. (2013). Kenyan banks face challenges with secure online transactions International banks are not as successful as in other markets. Available www.pcadvisor.co.uk.news/enterprise/3453739/Kenyan-banks-face-challenges with-secure-online-transaction/#ixzz27ieqP57.

Wechuli, a. On Cyber Security Assessment Framework; Case of Government Ministries in Kenya; International Journal of Technology in computer science and engineering, 1 (2014).

William K, R. and Guerra N. G. Prevalence and predictors of internet bullying. Journal of Adolescent Health, 41, S14-S21, (2007).

World ECONOMIC Forum (2011) The Mobile Financial Services Development Report 2011

Http://Www3.Weforum.Org/Docs/Wef_MFSD_Reoirt_2011.Pdf. Accessed 20 January, (2018).

Zeviar, G. The State of the Law on cyber jurisdiction and Cybercrime on the Internet, California Pacific School of Law, Gonzaga Journal of International Law, Vol. 1, (1998)