



**UNIVERSITY OF NAIROBI**

**INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES**

**CYBER TERRORISM AND NATIONAL SECURITY IN AFRICA: A CASE STUDY  
OF KENYA**

**ERIC K. LEE ROTICH**

**R50/35338/2019**

**A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENTS FOR THE AWARD OF MASTERS DEGREE IN  
INTERNATIONAL STUDIES FROM THE INSTITUTE OF DIPLOMACY AND  
INTERNATIONAL STUDIES, UNIVERSITY OF NAIROBI**

**JUNE, 2020**

**DECLARATION**

This project is my original compilation and has not been submitted for any award in any other University.

..... Date.....

**Eric K. Lee Rotich**

**R50/35338/2019**

National Defence College – Kenya and University of Nairobi

It is acknowledged that this project has been submitted by my official approval as the University supervisor.

..... Date.....

**Dr. S. Handa**

**Supervisor**

National Defence College - Kenya (NDC-K) and University of Nairobi

## **DEDICATION**

It is a pleasure dedicating this work to my family, friends, relatives and associates.

## TABLE OF CONTENTS

TITLE.....	i
DECLARATION.....	ii
DEDICATION.....	iii
TABLE OF CONTENTS.....	iv
ACKNOWLEDGEMENT.....	vi
ABBREVIATIONS.....	vii
DEFINITION OF TERMS.....	ix
ABSTRACT.....	x
CHAPTER ONE.....	1
INTRODUCTION TO THE STUDY.....	1
1.0 Introduction.....	1
1.1 Background of the Study.....	1
1.2 Statement of the Research Problem.....	3
1.3 Research Questions.....	4
1.4 Objectives of the Study.....	4
1.5 Literature Review.....	4
1.6 Theoretical Framework.....	9
1.7 Hypothesis of the Study.....	11
1.8 Research Methodology.....	11
1.9 Outline of the Study.....	12
CHAPTER TWO.....	13
NATURE OF CYBER-TERRORISM THREATS IN AFRICA.....	13
2.1 Background of Cyber Threats.....	13
2.2 The Nature of Cyber Threats.....	17
2.3 Consequences of Cyber-Terrorism Threats.....	21
2.4 Mitigation Measures against Cyber Threats.....	24
2.5 Chapter Summary.....	25
CHAPTER THREE.....	26
THE IMPLICATIONS OF CYBER TERRORISM THREATS TO NATIONAL SECURITY IN KENYA.....	26
3.1 Implications of Cyber Terrorsim Threats.....	26
3.2 Cyber Terrorsim on Critical Infrastructure in Kenya.....	30

3.3	Emerging Patterns of Cyber Technology as a National Threat.....	31
3.4	Kenya Cyber Security Measures and Strategies.....	34
3.5	Chapter Summary.....	35
	CHAPTER FOUR.....	36
	STRATEGIES TO COUNTER CYBER TERRORISM IN KENYA.....	36
4.1	Research Findings.....	36
4.2	Cyber Threat and National Security.....	44
4.3	The Emergent Patterns of Cyber Terrorism.....	48
4.4	Counter Cyber Security Measures and Strategies Applied.....	49
4.5	Chapter Summary.....	54
	CHAPTER FIVE.....	55
	SUMMARY, CONCLUSIONS AND RECOMMENDATIONS.....	55
5.1	Introduction.....	55
5.2	Summary.....	56
5.3	Conclusions.....	57
5.4	Recommendations.....	57
5.5	Suggested Areas for Further Studies.....	57
	REFERENCES.....	58
	APPENDICES.....	63

## **ACKNOWLEDGEMENT**

It is a pleasure to acknowledge my supervisor Dr. S. Handa and each and every person who has contributed to the success of this study. This research project was made a success through the help, cooperation and contribution of National Defence College.

## ACRONYMS AND ABBREVIATIONS

AS	Al-Shabaab
AT&T	American Telephone and Telegram Company
AU	African Union
AUC	African Union Commission
BFID	Banking Fraud Investigation Department
CAK	Communication Authority of Kenya
CPU	Central Processing Unit
CSI	Computer Security Institute
DDoS	Distribution Denial of Services
DoS	Denial of Service
EACO	East African Communications Organization
ECA	Economic Commission for Africa
FBI	Federal Bureau of Investigation
GDP	Gross Domestic Product
GPS	Global Positioning System
IBM	International Business Machines
ICT	Information Communication Technology
IDIS	Institute of Diplomacy and International Studies
IFMIS	Integrated Financial Management Information System
INTERPOL	International Police
IP	Internet Protocol
IT	Informational Technology
ITU	International Telecommunication Unit
KDF	Kenya Defence Forces
KDN	Kenya Data Networks
KE-CIRT/CC	Kenya National Computer Incidence Response Team Coordination Center
KIC	Kenya Information and Communication
KRA	Kenya Revenue Authority
LOIC	Low Orbit Ion Canon
MIT	Massachusetts Institute of Technology
NAVSTAR	National System using Timing and Ranging
NCIC	National Cohesion and Integration Commission
NDC-K	National Defence College – Kenya

NGO	Non Governmental Organizations
OECD	Organization for Economic Co-operation and Development
PKI	Public Key Infrastructure
SMS	Short Message Services
SPSS	Statistical Package for Social Science
SRI	Stanford Research Institute
TESPOK	Telecommunication Service Providers
UK	United Kingdom
UNODC	United Nations Office on Drugs and Crime
UON	University of Nairobi
USA	United States of America
USD	United States Dollars
WWW	World Wide Web



## DEFINITION OF TERMS

**Application** - this is computer software that performs a task or a given set of tasks of various types. In some instances applications can also be called programs.

**Cyber** - this is a general term denoting computers, information technology, and virtual reality, computer networks and relating to the internet.

**Cyber Security** - this denotes the theory and practice of defending computers from malicious ware and other dangers posed by various products, services, processes, procedures and practices made to protect devices, networks, data and other programs from any form of attacks, damage, destruction and or unauthorized access.

**Cyber Terrorism** - this is thought of as a phenomenon that involves the use of cyber space or the internet to carry out unlawful acts, that lead to possible violence, extremism, resulting in life being lost, property harm plus disruption of electronic systems with the aim of creating uncertainty, intimidation and fear in order to achieve ideological or political ends.

**Cybercrime** - this is also known as computer crime and it denotes the employment of computer systems as tools to advance various forms of illicit and disruptive activities.

**Nature of Cyber Terrorism** - this refers to the conduct involving computers, the internet and technology to advance religious, political and ideological ends, that are aimed at intimidation citizens, the state, governments, institutions or a section of the public.

## ABSTRACT

Technology in the World today has taken up all facets of life today than ever before. For instance Africa is rapidly developing and has become an increasingly technologically advanced in its Information Communication Technology (ICT) infrastructure. However, this advancement has also introduced a new challenge to many states. The research study objective was to examine cyber terrorism and national security in Africa through case study of Kenya. This is because the spread of technology has created some new vulnerability within the cyber domain that directly works to undermine national security. The susceptibilities of cyber space to attacks have grown without a corresponding defensive capability. The cybercriminals have developed an application that infiltrates and interfere with critical cyber technology infrastructure to obtain classified information and breaks bank accounts to steal money. This research employed quantitative and qualitative study approaches and the final field data source was eventually analysed Statistical Packages for the Social Science while qualitative data was analyzed using content analysis. The respondents who participated in this research included professionals in Information Communication Technology technical roles, security officers, financial institutions, academia, diplomats, legal institutions Information Technology and others. This research explored the measures and strategies applied in Kenya to safeguard the ICT sector against cyber threats. The study analyzed how cyber terrorism has on Kenya's national security. The research contextualized the concept of cyber security within the Securitization Theory in order to understand cyber technology and its effects to national security. This study found that cyber-attacks in Kenya have become prevalent and more serious to national security due to its porous nature and complexity. This research further found that the increase in cyber threats has been associated with computer use across various sectors of the economy which has attracted criminals to exploit the opportunities available. This research concludes that threats posed by cyber terrorism spreads especially with advancement of technology many cyber users have become vulnerable to online attacks and the threats can be overwhelming since they originate from anywhere on the globe. This section recommends that all government institutions shop protect their cyber systems against threats through the use of firewalls and antivirus software to curb the spread of malware in case a network is infected.

# CHAPTER ONE

## INTRODUCTION TO THE STUDY

### 1.1 Background to the Study

This chapter covers background information on technology. Technological information has highly impacted on each and every field from business, households, cooperation and governance. The twenty first century has been said to be the time that information and technology changed the security landscape in the world dramatically.

Lorenzo posits that the dimensions of cyberspace are wide since it has coverage that traverses from individual corporations, national health and international space.<sup>1</sup> It also includes sectors of security, diplomacy, industry and intellectual property. Cyber technology serves a crucial purpose when it comes to the global economy.<sup>2</sup> Hence the increasing use of cyberspace should be strong enough reason to encourage individuals, investors and governments to make cyberspace security a top priority.<sup>3</sup>

Brinkley and Fauth argue that everything is found in the cyber system and this turns the focus of both legal and illegal actions to cyberspace, some cyber activities include cybercrimes, cyber spying, hacktivism, cyber defense, cyber warfare, and cyber terror among others, which have potential to breach national security.<sup>4</sup> In the modern world, cyber insecurity presents a serious and unconventional threat. For instance, cyber terrorism has been serious to the United States of America (USA), since their economy and critical infrastructure depend on cyber systems to a big extent.<sup>5</sup> Thus security in the cyber domain is taken as a critical element in matters pertaining to national security that must be governed and explains the multibillion-dollar expenditure on protection of information systems and operations by various states.

According to Lewis the employment various cyber applications to cause damage, harm, disruption destroy key systems is considered a form of terrorism. These critical national infrastructures include electricity, hospital, airports and other state operations.<sup>6</sup> Thus cyber terrorism appears to be a very attractive avenue for causing disruptions by terrorists and

---

<sup>1</sup> Lorenzo, O. *Challenges of the Modern Century*, Samton Desktops Edition, Atlanta, Georgia, (2019), pp. 9-13.

<sup>2</sup> Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017), pp. 12-19.

<sup>3</sup> Ibid, (2017), p. 23.

<sup>4</sup> Brinkley, I and Fauth, R. *The Knowledge Economy*, United Kingdom, (2019), pp. 6-19.

<sup>5</sup> Lorenzo, O. *Challenges of the Modern Century*, Samton Desktops Edition, Atlanta, Georgia, (2019), p. 15.

<sup>6</sup> Lewis, J. *Cyber Threats and Cyber Wars*, Washington DC, (2012), pp. 3-9.

extremist.<sup>7</sup> Cyber terrorism comes in the wake of the fact that in Africa, violent extremism and terror groups have spread their tentacles electronically, therefore posing a grave danger to national security amongst many states.<sup>8</sup>

The United Nations (UN) defines cyber terrorism as a concept has no universally accepted definition at the moment. The point of contention is the fact that the concept includes a combination of many other ideas such as hacktivism and the use of the internet to spread terror.<sup>9</sup> Chow states that broadly speaking, cyber terrorism can be considered an attack on a major computer system with the ultimate aim of causing serious political, physical, economic, social, psychological and environmental harm.<sup>10</sup>

The cyber-attacks in East Africa are continuously evolving and becoming more dynamic.<sup>11</sup> Kenya has a robust technological infrastructure and therefore carries out her important activities in the fields of social, economic and national security.<sup>12</sup> This research aims at bridging the gap in appreciating the emerging problems of cyber terrorism and its effect on national security.

---

<sup>7</sup> Ibid, (2012), p. 11.

<sup>8</sup> Young, J. *The Twenty Four Hour Professor*. The Chronicle of Higher Education, 48, (2016), pp. 31-34.

<sup>9</sup> The United Nation. United Nations *Global Counter Terrorism strategy*. UN, United States, (2016), p. 21-29.

<sup>10</sup> Chow, S. *Security Alert Texas through Mexico*, Houston Texas, (2018), pp. 31-34.

<sup>11</sup> Ibid, (2018), p. 35.

<sup>12</sup> The Government of Kenya. *CBK Guidance on Cyber Security*, Nairobi, (2017), p. 3.

## **1.2 Statement of the Problem**

It is worth mentioning from the onset that increasing spread of cyber threats, cyber dangers and cyber-attacks in Kenya already is seen as an eventuality towards a serious national security threat. This has been made worse by the fact that critical infrastructure in the country are more vulnerable to cyber-attacks owing increased cyber connectivity, hence cyber terrorists can stage attacks resulting in disruption of systems.

In Kenya the potential of cyber terrorism is undeniable, especially since infrastructure is being automated. Some of them are technology base infrastructure, medical systems, and telecommunication, financial and electric grid, which terrorist will probably use technology to propagate attacks. This means that at the moment Kenya's critical national infrastructure is under serious threat of cyber-attack. Kenya has tried to create national strategies and policies that address cyber terror counter measures. For instance, Kenya in 2014 gave birth to the Kenya national security strategy with the aim of raising cyber security awareness and public empowerment particularly at workforce and citizens in Kenya to address growing cyber security needs.

In Kenya, the counter terror approaches put in place over the last decade have been geared towards traditional forms of terrorism and hence there is a need for detection, preventing and countering cyber terrorism. Noting the importance of sufficient security for critical state infrastructure, it is crucial to mitigate cyber terrorism and national security, as any disruption, destruction and instability in national security of these infrastructure results in grave consequences for the state and its social, political, economic and environmental situation. It is for these reasons that the research undertakes to better understand the nature, implications of cyber terrorism and further asses the measures to mitigate the problem of cyber terrorism in Kenya.

### **1.3 Objectives of the Study**

The general objective of this study is to examine cyber terrorism and national security in Africa through the case of Kenya. This study further specifically intended;

- 1.3.1** To assess the nature of cyber terrorism threats in Africa
- 1.3.2** To determine the implications of cyber terrorism threat to national security in Kenya
- 1.3.3** To examine the strategies and measures employed to counter cyber terrorism in Kenya

### **1.4 Research Questions**

- 1.4.1** What is the nature and extend of cyber terrorism in Africa?
- 1.4.2** What are the implications of cyber terrorism threat to national security in Kenya?
- 1.4.3** What are the strategies and measures employed to counter cyber terrorism in Kenya?

### **1.5 Literature Review**

This section is made of the literature review which consist mainly reviewed scholarly materials, that consists of journals, books, articles and periodicals. In this section many scholars have made attempts to demystify the subject of cyber space and national security. In addition, sub sections reviewed the theoretical and empirical literature relating to cyber terrorism threat to national security.

Cyber generally denotes things to do with computers, information technology, and virtual reality, computer networks and relating to the internet. The cyberspace generally connotes the interaction of key communication systems, data bases, source information, or bits into a vast electronic interchange. Network system is considered virtual and is created or becomes existent where there exist telephone wires and fiber optic lines.<sup>13</sup> Cyberspace has the grave potential to facilitate unlawful activities via for instance encrypted smart phones being used to disseminate extremist ideas, views and action.

Cyberspace is not only virtual but it also arises from computers, servers, satellites and cables among others.<sup>14</sup> In popular studies scholars interchangeably use terms like internet, cyberspace and web to mean the same thing.

---

<sup>13</sup> Lewis, J. *Cyber Threats and Cyber Wars*, Washington DC, (2012), p. 11.

<sup>14</sup> Young, J. *The Twenty Four Hour Professor*. The Chronicle of Higher Education, 48, (2016), pp. 31-34.

According to the United Nations, at the moment cyber attacks could be carried out through the use a wide range of tools, modes and approaches, some of which are popularly known as malware attacks, in the form of viruses and worms. It is important to appreciate that computer programs that duplicate themselves are known as *Trojan horses*. The types which usually duplicate themselves are intended to annoy or inconvenience ICT users. They can also compromise information confidentiality and integrity. The *Trojan horses* are programs that deceive applications and can be used to destroy information.<sup>15</sup>

The seriousness of the impact of damage or the threat the intruder will pose will depend on the value of degree or sensitivity of the information. Informal networks have been in existence from the 90s when the World Wide Web came into being. They have however rapidly grown in number from 2003 onwards. The reason for this growth includes the tremendously expanded storage capacity of data and the relative drop in the cost of storage and retrieving of information.<sup>16</sup> It is generally accepted that no individual or government can ignore the rapid growth and development of the Web 2.0 and its global reach, plus spread which is ever expanding and the high potential it possesses in its use in enhancement of new technologies and social networking.<sup>17</sup> For instance the online social media and other social networks have affected each and every aspect of human endeavor from the health, environmental, ecological, political, economic, cultural, psychological, and all the way to national safety and security.

According to Riis the concept of cyber terrorism is considered the employment of computer systems to perpetrate threatening acts.<sup>18</sup> The importance of networking security is becoming a greater than it was in yester years due to the fact that the interconnectedness of the global village exposes large amounts of information which is personal, governmental or commercial type of information to threats.<sup>19</sup> Dowd and McHenry posit that information technology has been dominated by two broad types of networks, that is, data networks and synchronous networks.<sup>20</sup> These networks are thought of as digital telecommunication systems which enable the sharing of data information.

---

<sup>15</sup> Lewis, J. *Cyber Threats and Cyber Wars*, Washington DC, (2012), p. 14.

<sup>16</sup> Lorenzo, O. *Challenges of the Modern Century*, Samton Desktops Edition, Atlanta, Georgia, (2019), pp. 7-19.

<sup>17</sup> Ibid, (2019), p. 93.

<sup>18</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

<sup>19</sup> Ibid, (2019), pp. 121.

<sup>20</sup> Dowd, T and McHenry, C. *Security of Networks and the Time to act*, Continental review, (2008), p. 23.

According to Lewis one of the most popular data network systems is the internet that is usually composed of routers.<sup>21</sup> The information stored can be accessed and obtained by planting specifically manufactured programs or applications like the ‘Trojan horses’ in to the system.<sup>22</sup>

Yunos and Salman argue that adopting the framework of securitization theory, specifically the securitization of cyberspace has found that governments have since recognized serious risks in cyberspace. The genesis of online breach and damage debate goes back to the Regan white house whose office was once concerned with the potential risk of classified information disclosure.<sup>23</sup> Cyber Security forums were used by computer experts in the late part of the last century to point out vulnerabilities to networked computers.<sup>24</sup>

The phrase “Cyber-terrorism” is believed to be first used by Barry Collin.<sup>25</sup> No one definition is considered to be the official definition.<sup>26</sup> Defining cyber terrorism is a tricky affair since it’s difficult in establishing the intention, identity, or political motivation of an attacker with certainty.<sup>27</sup> It is crucial to be aware that the word cyber-terrorism is being used more frequently in recent times, yet a single definition of the concept has remained elusive, as the phrase is loosely defined, as a concept, it tends to be a subjective one.<sup>28</sup> Chuipka argues that the convergence between the digital and physical world, result in some kind of vulnerability.<sup>29</sup> The computer and the internet are each considered as a distinct attribute.<sup>30</sup> Such methodology is used to better understand the online computer terrorist. This is because the traditional assessment of online terrorism as being mainly targeting the computer is passé as it only touches on a fraction of what the entire concept entails.<sup>31</sup>

---

<sup>21</sup> Lewis, J. *Cyber Threats and Cyber Wars*, Washington DC, (2012), p. 19.

<sup>22</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

<sup>23</sup> Young, J. *The Twenty Four Hour Professor*. The Chronicle of Higher Education, 48, (2016), pp. 31-34.

<sup>24</sup> Ibid, (2016), p. 37.

<sup>25</sup> Buzan, B. *Rethinking security after the Cold War*, International Security Studies, (1997), p. 91-91.

<sup>26</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

<sup>27</sup> Ibid, (1997), p. 21.

<sup>28</sup> Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017), pp. 12-19.

<sup>29</sup> Chuipka, A. *The strategies of Cyber terrorism*, Graduate School of public and International Affair, University of Ottawa, (2016), pp. 5-9.

<sup>30</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

<sup>31</sup> The United Nation. United Nations Global Counter Terrorism strategy. UN, United States, (2016), p. 23.



Cyber-terrorism is the use of digital technologies in a way that proves to be insidious to the national interests of a country.<sup>32</sup> This kind of threat is considered by experts to be even more dangerous than the typical form of terrorism.<sup>33</sup> This is because through cyber terrorism large sectors of a country's economy or the workings of government can be interfered with, such as government records, air traffic control, damming systems, medical records and many other crucial sectors.<sup>34</sup> The ripple effects from this may lead to a very serious threat to national security and greater loss of assets. In addition it could also affect consumer confidence and even lead to loss of life in the event of hacking of medical networks.<sup>35</sup>

Young thoughts are rapid technological developments have created many avenues of new opportunity and potentiality for efficiency for all sizes and types of organizations; they have equally presented unprecedented threats and vulnerabilities. Cyber security usually involves systems protection, networks, cyber and data in the cyber realm.<sup>36</sup> Cyber security relevance increases when many devices are connected online.

The Communication Authority of Kenya (CAK) has sounded the alarm over the potential of the increasing cases of cyber terror attacks in the state. Thus it was said that, "Cyber security is about the security online and the processes that create a secure environment online."<sup>37</sup> The Serianu Cyber Security Report shows that the cost of cyber-crime in Africa has exponentially increased to about of 3.5billion US dollars; Nigeria (\$649million), Kenya (\$210million), Tanzania (\$99million), Uganda (\$67million), and Ghana (\$54million).<sup>38</sup> This is as automation keeps taking place in many sectors of the economy, the cost keeps growing.<sup>39</sup> In some cases, like Kenya, electronic services have proven to be vulnerable to attack to the private and public since a lot of money has been lost in recent years due hacking.<sup>40</sup> This was mainly due to lack of sufficient technology security expertise.<sup>41</sup>

---

<sup>32</sup> Chuipka, A. *Strategies of Cyber Terrorism: Is Cyber terrorism*, Ontario, Canada, (2016), pp. 89-91.

<sup>33</sup> Ibid, (2016), p. 93.

<sup>34</sup> The United Nation. *United Nations Global Counter Terrorism strategy*. UN, United states, (2016), p. 23.

<sup>35</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

<sup>36</sup> Young, J. *The Twenty Four Hour Professor*. The Chronicle of Higher Education, 48, (2016), pp. 31-34.

<sup>37</sup> Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017), pp. 12-19.

<sup>38</sup> Lewis, J. *Cyber Threats and Cyber Wars*, Washington DC, (2012), p. 19.

<sup>39</sup> Ibid, (2012), p. 21.

<sup>40</sup> Nixon Kanali is a trained journalist based in Nairobi. Also founder and editor of Tech Trends KE, (2016).

<sup>41</sup> Ibid, (2016).

The Kenya Cyber Security Policy is presently coordinated by CAK.<sup>42</sup> Key tenets of the policy are computer access training and awareness cyber safeguards and policies and ICT economic drivers, ICT governance and legal framework.<sup>43</sup> Through these strategies several teams have been established to oversee implementation of cyber technology and security measures such as anchored in the law.<sup>44</sup> Recognizing the importance of ICT, the crime unit the police and the Communication Authority of Kenya, all have a branch devoted cyber security crimes under the law.<sup>45</sup>

Kenya has gone ahead to develop strategies to respond to the rising cyber security threats by adapting to internationally recognized standards.<sup>46</sup> Recognizing the importance of ICT in economic development, Kenya has chosen to seek partnerships with actors in the digital world to develop a strategy based on their experience on the risks.<sup>47</sup>

Kigen and Mchai argue that align with the agenda requirements of the global cyber security, the KECIRT/CC is responsible for providing advisory role on national security in the cyber domain and cyber incident reporting systems working in conjunction with stakeholders at the local, regional and international levels.<sup>48</sup> However, KECIRT/CC lacks requisite capacity in skill as well as inadequate resources to fully engage with the partners; in looking at it is likely to lose its meaning in the industry.<sup>49</sup> As the uptake of technology increases in virtually every industry in Africa, the hunting fields for cyber terrorists has also expanded exponentially, thus making cyber terror attacks potentially even more common.

The Kenya National Cyber Security Master Plan 2018/19 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 enable economic growth.<sup>50</sup>

---

<sup>42</sup> Kigen, P and Mchai, C. *Kenya cyber security report*, (2014), pp. 91-95.

<sup>43</sup> Ibid (2014), p. 103.

<sup>44</sup> Lorenzo, O. *Challenges of the Modern Century*, Samton Desktops Edition, Atlanta, Georgia, (2019), pp. 9-13.

<sup>45</sup> Newton, B. *Phone Scams of Millions*. Survey of Cyber Crimes in Kenta, Tanzania and Zambia, Herald Cooperation, (2014), pp. 9-11.

<sup>46</sup> Nixon Kanali is a trained journalist based in Nairobi. Also founder and editor of Tech Trends KE, (2016).

<sup>47</sup> Ibid, (2014), pp. 12-16.

<sup>48</sup> Kigen, P and Mchai, C. *Kenya cyber security report*, (2014), pp. 91-95.

<sup>49</sup> Kigen, G. *Kenya cyber security report 2014*, (2014), pp. 3-7.

<sup>50</sup> Fischer, E. *National Framework for Cyber Security*, SCR Report for Congress, Order Code, (2015), p. 23.

In addressing of cyber threats has been achieved by enacting the Kenya Information and Communication (KIC) Act of Cap 411A which was amended into ICT Act, 2014 and establishes an authority that provides some kind of certification authority, whose intent is to, “give give a media for infrastructure development and working framework for cyber security bodies.”<sup>51</sup> National strategies aim to assist in making Kenya improve the current cyber security posture and provide guidance on how to secure cyber infrastructure against threats.<sup>52</sup>

The Kenya government has recognized the need to establish a cyber-coordination Centre where all cases of attack on critical ICT infrastructure can be reported.<sup>53</sup> In addition the act known as computer misuse and cyber Act of 2018 is useful for developing forensic procedures when cases of cybercrimes occur.<sup>54</sup> In reviewing the literature this study found gaps to the effect that cyber insecurity is a global responsibility and needs attention of the state.<sup>55</sup> It is critical to appreciate that in reviewing the literature, this section argues that security challenges in developing states seem to have a common approach, and setups for these developing states have shortcoming and they continue to evolve and sheds light on how Africa states.

## **1.6 Theoretical Review**

### **1.6.1 Theory of Securitization**

This study employed the theory of securitization as formulated by Ole Weaver which has become common among the constructivist studies in the discipline of International Relations (IR). Securitization is the process of the state transforming subjects into general security matters.

According to Buzan, security is what primarily moves politics and depending on the seriousness of the situation it can be used as an extraordinary factor that may need state actors to apply special powers that are usually beyond the scope of the conventional law.<sup>56</sup> The securitization of a particular issue involves a process that goes beyond the normal political

---

<sup>51</sup> Lewis, J. *Cyber Threats and Cyber Wars*, Washington DC, (2012), p. 6.

<sup>52</sup> Fischer, E. *History of Critical Infrastructure*, Atlanta Georgia, RL3, (2015), p. 227.

<sup>53</sup> The East African. *Kenya launches centre to fight cybercrime*, (2016).

<sup>54</sup> Lewis, J. *Cyber Threats and Cyber Wars*, Washington DC, (2012), p. 5.

<sup>55</sup> Libichi, B. *Cyber deterrence and Cyber Wars, Laws of Cyber Space*, Atlanta Georgia, RL3, (2018), p. 229.

<sup>56</sup> Buzan, B. *Rethinking security after the Cold War*, International Security Studies, (1997), p. 91-91.

means to resolve the threat that the issue presents.<sup>57</sup> Within the securitization theory, the term threat is critical as it determines the existential nature that is behind the move to securitize an issue in order to make it exceptional.<sup>58</sup>

Theorists of securitization argue that successfully securitized objects are endowed disproportionately on amounts of attention and resources juxtaposed to unsuccessfully securitized subjects resulting in more human damage.<sup>59</sup> A good example is the kind of funding and precedence that the topic of terrorism consumes even though people will die as a result of automobile accidents or even malaria than from the results of terrorism.<sup>60</sup>

The key attribute to preventing cyber terrorism is awareness because all a cyber-terrorist looks for is access into a network and one could just be providing them with it through poor cyber hygiene.<sup>61</sup> Analysts are raising fears that the increased frequency of terror attacks may negatively affect the economy in the long run.

This research notes that until recently, in Kenya terrorism has been linked to physical acts of crime and violence, example, bombings and destruction of property. From the advent of early years of the 1990s with the rapid evolution of computer technologies, new forms have emerged, many of them taking place within the cyber space.<sup>62</sup>

The key element to preventing cyber terrorism is awareness because all a cyber-terrorist is looking for is access to a network and you could just be providing them with it through simple careless habits.<sup>63</sup> The reach and impact of cyber terrorism is accelerating and becoming more complex for governments to solely address. This research therefore tries to address the need for increased awareness of internal (national) cyber threats.

---

<sup>57</sup> Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017), pp. 12-19.

<sup>58</sup> Libichi, B. *Cyber deterrence and Cyber Wars, Laws of Cyber Space*, Atlanta Georgia, RL3, (2018), p. 229.

<sup>59</sup> Ibid, (2018), pp. 231-232.

<sup>60</sup> Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017), p. 21.

<sup>61</sup> Nixon Kanali is a trained journalist based in Nairobi. Also founder and editor of Tech Trends KE, (2016).

<sup>62</sup> Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017), pp. 12-19.

<sup>63</sup> Libichi, B. *Cyber deterrence and Cyber Wars, Laws of Cyber Space*, Atlanta Georgia, RL3, (2018), p. 229.

## **1.7 Hypotheses of the study**

- 1.7.1** The nature of cyber-terrorism threats in Africa is misunderstood
- 1.7.2** The lack of awareness has led to high incidents of cyber terrorism in Africa
- 1.7.3** The counter cyber terrorism strategies and measure employed in Kenya have a multi-agency approach.

## **1.8 Research Methodology**

This study applied case study as a research design. It is important to appreciate that case studies are usually executed in the subject's real-world context, which allows the researchers a non-biased view of what they are. This research utilized primary and secondary data sources; in addition it applied qualitative and quantitative approaches to critically examine cyber terrorism and national security in Africa using Kenya.

The mix of both qualitative and quantitative research has advantageous since it enhanced the results of findings and conduct of the excellent educational research. Combining qualitative and quantitative approaches enhanced the evaluation. It ensured a balance between the limitations of various data with the strengths of others. The cats of cyber terrorism transcended global, regional, national and local boundaries. There this study was done in the whole of Kenya, but with a sharp focus on Nairobi County. The target population was practitioners in terrorism and national security.

The respondents included structured questionnaire was aimed at key stakeholders in cyber security who included, Kenya Defense Forces, National Police Services, National Counter Terrorism Center, Immigration Department, Kenya Prison Service, Kenya Civil Aviation, Ministry of Foreign Affair, National Intelligence Service.

The sample size is crucial to whatever study because this allows the researcher to make appropriate inferences of a population sample. This helped in removing bias on the samples chosen. Such biases would likely negatively affect the quality of data and the resultant study findings of this research the primary data was gathered from interviews. The qualitative data are collected by researchers through interviews.

This study used key informant interview guide and focus groups. The focus group discussion involved the Sub County Security Committee. In addition, secondary data was collected from

cyber security related sources such as, books, journals, articles and periodicals. This helped capture precise information that made it possible to generate new insights or simply verify and confirm from previous analyses on cyber terrorism.

In order to guarantee validity and reliability this research harnessed the research instrument through repeatability which in turn enhanced its internal consistency, during this exercise the tools for research will be tested beforehand. A pilot sample analysis of the research tool was done to observe if the outcome in line with study objectives.

The collected data was organized and analysis done on it by document and theme analysis, from upcoming issues that arose from the research. The definition of thematic analysis is that it is a method of quality that is usually used for recognizing themes in a data set. It is worth noting that a theme is a repeating pattern that can be observed within a set of data under predefined conditions. Emerging results was finally presented in narrative, frequency tables, bar graphs and pie chars. This study was undertaken in Nairobi County, with a focus on the most affected constituencies within the City. In addition, this was undertaken in 2020.

## **1.9 Study Outline**

Chapter one makes up the introduction. The study lays makes a theoretical framework of the issues to be addressed and particularly, what is to be investigated. Chapter two illustrates the forms, nature and status of strategies and infrastructure for countering cyber terrorism, and shows how the cyber terrorism impacts the whole of society, to make it very clear that everyone has a part to play in our national response. Chapter three gives clear implications of cyber terrorism threat to national security in Kenya. Chapter four gives the strategies and measures employed to counter cyber terrorism in Kenya and it further explores the cyber terrorism security connection in Kenya. Chapter five finally sums up the research study and hypotheses. It makes conclusions and recommendations on the way forward.

## CHAPTER TWO

### NATURE OF CYBER TERRORISM THREATS IN AFRICA

#### 2.1 Background of Cyber Threats

Hacking involves the unlawful access into a computer network by either a person or an intelligent piece of software that has been unleashed online. In the beginnings of the internet many hackers broke into networks just for fun but with time the motivation has become financial and or even political. Information technology has made computers both the target and originators of attacks on networks or even personal computers.<sup>64</sup>

A critical challenge that is facing the world today is the harmonization of cyber laws across not only different countries but also different regions of the world.<sup>65</sup> There have been numerous cases of computer system abuse in history that warrant action. In the years 1969 college students in Montreal Canada began rioting when authorities were called in to quell occupation by students of several floors of the Hall building. The cost of the whole affair was in the range of two million dollars, 97 people were arrested.<sup>66</sup> It is critical to appreciate that Thomas Whiteside documented a string of cases involving actual physical attacking of computer systems during the 1960s and 70s.<sup>67</sup> In 1968 in Olympia Washington, a man with a pistol shot twice into an IBM computer. In 1970 the University of Wisconsin an explosion killed one. In 1970 at the Fresno State College Molotov cocktails were used and caused about one million US dollars damage to computer systems.<sup>68</sup>

An expensive magnetic core was damaged in 1972 in New York inside a Honeywell computer, the damage was made by an individual using a sharp object resulting in damage that amounted to about a million United States dollars.<sup>69</sup> In 1973 at Melbourne in Australia, Antiwar protesters shot into a computer belonging to an American firm using a double-barreled shotgun while in 1974 at Charlotte, North Carolina a frustrated computer operator at the Charlotte Liberty Mutual Life Insurance Company shot into the computer. The internet first came to be in the 1960s, it was made possible by the development of packet

---

<sup>64</sup> Nixon Kanali is a trained journalist based in Nairobi. Also founder and editor of Tech Trends KE, (2016).

<sup>65</sup> Seymour, B, Kabay, E and Eric, W. *Computer Security Handbook*, 5<sup>th</sup> Ed, John Wiley Inc, New Jersey, (2009), p. 3.

<sup>66</sup> Ibid, (2009), pp. 6-8.

<sup>67</sup> Wilson, D. *Internet Awareness and Dangers*, Atlanta University, United States of America, (2016), p. 5.

<sup>68</sup> Nixon Kanali is a trained journalist based in Nairobi. Also founder and editor of Tech Trends KE, (2016).

<sup>69</sup> Ibid, (2016).

transmission whereby data is broken into small<sup>70</sup> portions and each portion of the data is encoded with *meta* data in order to be self-descriptive to the network. This technology was developed by a student of MIT who went by the name Klyanrokom.<sup>71</sup>

In the 1960s the internet was mostly used by the military and a few scientific institutions and the main risks involved in networking of computers back then was the loss of sensitive information, but it seems that today the risks have grown many times over. The development of technology has not only put computer networks at a possible loss of losing information but also corruption of data.<sup>72</sup> It is part of the human condition that criminality is part of any society and therefore it is only logical to be vigilant on the cyberspace since criminality is present there too and with every advancement of computer technology, the cyber criminals are getting more and more sophisticated and the frequency of cyber-crime also increases.<sup>73</sup> Definitive data for computer crimes is usually not consistent across different studies because many a time the victims of these crimes are unaware they have even taken place.

The pioneer of fighting computer crime was Donn B. Parker, a citizen of the United States. He started this work back in the 1970s.<sup>74</sup> He served as a security consultant on matters of Stanford Research Institute (SRI).<sup>75</sup> He wrote the manual for enforcement of cyber laws and it became even popular internationally.<sup>76</sup> In Holland, H. W. K. Kaspersen an academician, was involved in fighting computer crime and later became the head of the Council of Europe Cybercrime Convention.<sup>77</sup> Over the period of time, with the ever-evolving sophistication of computer system linked technologies, crimes have changed their nature and color too. Incidences of hacking first started appearing in the 1980s. A good example was the hacking of AT&T computer system which made customers get discounted rates on their phone bills.<sup>78</sup>

---

<sup>70</sup> Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017), pp. 12-19.

<sup>71</sup> Nixon Kanali is a Trained Journalist based in Nairobi. Also Founder and editor of Tech Trends KE, (2016).

<sup>72</sup> Ibid, (2016), p. 31.

<sup>73</sup> Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017), pp. 12-19.

<sup>74</sup> Matinde, V. *High Data Cost and Factors of Mobile Insecurity in Africa*. IDG Connect, (2014), p. 14-15.

<sup>75</sup> Shrekiam, E. *Cyber Crime in North Africa, the Shape of Future Conflicts*, Journal of Crime, (2015), p. 7.

<sup>76</sup> Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017), pp. 12-19.

<sup>77</sup> Ibid, (2017), p. 23.

<sup>78</sup> Matinde, V. *High Data Cost and Factors of Mobile Insecurity in Africa* IDG Connect, (2014), pp. 14-15.



In the 1990s credit card fraud and identity theft emerged and it caused serious losses to many companies.<sup>79</sup> A one John Draper, who had the alias of Captain Crunch, fooled the AT&T networks by simply using a plastic whistle and a box of breakfast cereal.<sup>80</sup> Kevin Mitnick became a wanted man by the FBI for hacking into academic and corporate computer systems and in the process causing millions of dollars' worth of damage to these institutions. He managed to elude the authorities for decades but was finally captured in the 1990s and ended up spending five years in jail and was banned from using a computer for three years after his release.<sup>81</sup> In the late 1990s the "Mellissa" and "I love you" viruses caused a lot of damage that the emergence of anti-virus software sprung up in the market. It is now a multi-billion-dollar industry.<sup>82</sup>

Leverett posits that there is a form of hacking which is called Denial Of Service (DOS) which essentially is flooding a particular network with so much outside information to the point it crashes. They can be very costly as was seen in the year 2000 in Canada where a fifteen-year-old boy invoked such an attack on numerous e-commerce sites which shut them down. By the time the problem was solved, over a billion dollars was lost.<sup>83</sup>

Matinde argues that in 2007 what was believed to be Denial of Service, by Russian agents crippled the digital infrastructure of Estonia. This was after there was a diplomatic row between the two countries when Estonia decided to remove two world war two Russian soldier statues from a public area. The attack paralyzed the media, government and the banking system.<sup>84</sup> In the brief military altercation between Russia and Georgia a few years ago, it is believed that the Russians crippled the digital infrastructure of the country through hacking. It disrupted cell phone services and the banking sector.<sup>85</sup>

Africa has not been spared this scourge of cyber-crime. Just recently the authorities discovered a ring of hackers that were extracting information from people's social media accounts and even from their financial institutions' records and were using this

---

<sup>79</sup> Ibid, (2014), p. 21.

<sup>80</sup> Kigen, G. *Kenya cyber security report 2014*, (2014), pp. 3-7.

<sup>81</sup> Nixon Kanali is a Trained Journalist based in Nairobi. Also Founder and editor of Tech Trends KE, (2016).

<sup>82</sup> Matinde, V. *High Data Cost and Factors of Mobile Insecurity in Africa*. IDG Connect, (2014), pp. 14-15.

<sup>83</sup> Shrekiam, E. *Cyber Crime in North Africa, the Shape of Future Conflicts*, Journal of Crime, (2015), p. 7.

<sup>84</sup> Matinde, V. *High Data Cost and Factors of Mobile Insecurity in Africa*. IDG Connect, (2014), pp. 14-15.

<sup>85</sup> Lewis, J. *Risk of Cyber Terrorism*, Center for Strategic Studies and International Studies, Washington DC, United States of America, (2018), pp. 30-32.

information for leverage, they were innocuously calling it, data mining..<sup>86</sup> This means local cyber intelligence teams need to be recruited.<sup>87</sup>

It seeks to provide funding for the security agencies to have necessary forensic tools to fight cyber-crime which in 2013 alone, is estimated to have cost the country over two billion Kenya shillings.<sup>88</sup> This piece of legislation is the product of long discussions in 2004 between TESPOK and cyber experts from Canada, India, Singapore and South Africa on how to fight cyber-crime.<sup>89</sup> In Kenya, on July 2014, Article 19 analyzed the first draft of the Cybercrime and Computer related Crimes Bill in Kenya ('Cybercrime Bill').<sup>90</sup> This bill originated from the office of the (DPP). The result was a resolution that the country needed a comprehensive cyber crime law that will fill the gaps left by the existing legal framework.

## **2.2 The Nature of Cyber Threats**

This section acknowledges from the onset that cyber threats are a rapidly growing vice in Africa today than ever before. The threats are growing as the perpetrators become more sophisticated with each passing day as the technology advances. The emerging cyber threat trends in Kenya present in form of malware which is known to be a malicious software attack that causes harm to computer users and their system.<sup>91</sup>

The malware can manifest in form of viruses or worms that enter into the computer software without the user's knowledge and detection.<sup>92</sup> These attacks may include Botnet attacks, mobile malware attacks, phishing or password sniffing and Distribution Denial of Service (DDOS).

According to Serianu the growing number of broadband and fast internet connection, increases the number of botnets attacks in Kenya.<sup>93</sup> In the years 2013 the cases of botnet

---

<sup>86</sup> Ibid, (2018), p. 37.

<sup>87</sup> Matinde, Vincent. High Data Cost and Factors of Mobile Insecurity in Africa IDG Connect, (2014), pp. 14-15.

<sup>88</sup> Ibid, (2014), p. 19.

<sup>89</sup> Nixon Kanali is a Trained Journalist based in Nairobi. Also Founder and editor of Tech Trends KE, (2016).

<sup>90</sup> Shrekiam, E. *Cyber Crime in North Africa*, the Shape of Future Conflicts, Journal of Crime, (2015), p. 7.

<sup>91</sup> Matinde, Vincent. High Data Cost and Factors of Mobile Insecurity in Africa IDG Connect, (2014), pp. 14-15.

<sup>92</sup> Shrekiam, E. *Cyber Crime in North Africa*, the Shape of Future Conflicts, Journal of Crime, (2015), p. 7.

<sup>93</sup> Matinde, V. *High Data Cost and Factors of Mobile Insecurity in Africa*. IDG Connect, (2014), p. 17.

attacks detected grew by 100 per cent from 900,000 events to 1,800,000 between the years 2012 to 2013.<sup>94</sup> This increase is attributed to the advancement in the internet connectivity coupled with unprotected computers which easily attract cyber criminals and illicit cyber activities. The attackers take advantage of this situation to attack identified infrastructure such as financial institutions and government offices with a view to defraud, cripple or steal information.<sup>95</sup>

It is a worrying trend in Kenya when reports from the BFID show that about 300 million US dollars was electronically stolen between 2015 and 2016 and yet only 10 million US dollars was recovered.<sup>96</sup> This was done in various ways like through identity theft, electronic fund transfers, credit card fraud and online forgery of documents.<sup>97</sup>

The malware attacks are mostly common and are relatively easy to execute and has substantial effect on the target. Often, the perpetrators of these attacks use computer programs network tools referred to as Low Orbit Ion Cannon (LOIC) and target a specific website or network. These stress tools work in the form that it overload's the server with of the target with large data hence temporarily disconnecting the network.<sup>98</sup> Another method or technique is the Distributed Denial of Service Attack (DDoS) which use similar principles as LOIC but on a bigger scale by attacking several computers in a botnet hence intensifying the effects.

The LOIC network stress is easy to use as it can be downloaded and administered by people with limited computer knowledge and programming skills. The DDoS attacks are very prevalent because of growing new online services which are developed each day. They include hackers who target banks and Anonymous actors such as viruses or Worms. The prominence of this attack has been necessitated by the lack of use of antivirus to clean up the system.<sup>99</sup> As Kenya continues to embrace online enabled services such as 1-tax System.

---

<sup>94</sup> Serianu. Kenya Cybersecurity Report 2014. Rethinking cyber security An Integrated Approach: Process, Intelligence and Monitoring, (2014), p. 8.

<sup>95</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>96</sup> Kamande, W. *The Cyber Crime Society*. Journal of Alternative Perspectives in Research, (2013), p. 89.

<sup>97</sup> Matinde, V. *High Data Cost and Factors of Mobile Insecurity in Africa*. IDG Connect, (2014), p. 21.

<sup>98</sup> David, W. *Cybercrime, the Transformation of Crime in the Information Age*, Polity, (2007), p. 27

<sup>99</sup> MacAfee 2014, MacAfee Labs Threats Reports. June 2014.

Ken-Trade single window system and Integrated Financial Management Information System (IFMS), such as e-infrastructure have become susceptible to DDOs attacks.<sup>100</sup> According to CSI Comp Crime Survey, (2010/2011) surveys malware attacks account for 67.1 per cent in Kenya cybercrimes<sup>101</sup> Malware attacks manifest in the form of malicious worms mutating programs that contaminate computers and spread quickly through networks and the internet.

According to MacAfee, 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<sup>102</sup> Considering that over 50% of people in Kenya own a cellular device, mobile malware poses a substantial threat as they access internet services using their mobile phones.

This section argues that social Media are links characterized by extremely cheap global mode of communication.<sup>103</sup> The platform has huge impact on social and security implications for the Kenya people and the government. Social media is a term used to refer to the group of technologies related with fast information distribution via vastly available web-based platforms.<sup>104</sup>

It represents an important change of broadcast media into multiple community dialogues, featuring the Web 2.0 revolution of the Internet. “Web 2.0” represents an essential shift across the Internet use in the modern twenty first century, which has transformed communication network in which every user has the ability to produce and consume.<sup>105</sup> Examples of Web 2.0 social media include, Facebook and Myspace, eBay reputation Flickr, YouTube, Google Maps and Twitter. Social media is a 21st century emerging communication technology that started in the United States 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, families, corporations and organization. The platform is now used to

---

<sup>100</sup> Shrekiam, E. *Cyber Crime in North Africa*, Shape of Future Conflicts, Journal of Crime, (2015), p. 7.

<sup>101</sup> Ibid, (2015), p. 39.

<sup>102</sup> MacAfee 2014, MacAfee Labs Threats Reports. June 2014.

<sup>103</sup> Ibid, (2014).

<sup>104</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>105</sup> Leverett, E. *Cyber Terrorism: Assessment of the Threat to Insurance*, Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge, (2017), pp. 12-13.

perpetrate crime in most parts of the world including Kenya.<sup>106</sup> These attacks present in the form of defamatory hate speech, cyber bullying and terrorism.

Hate speech is a complex nexus between freedom of expression and dignity. Hate speech has been 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 use. 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.<sup>107</sup>

On July 2014 the Kenyan government experienced a number of attacks by hacktivists. One of them was on the Kenya Defence Forces (KDF) twitter account where a lot of unsavory messages were posted. The force's spokesman account was also hacked and the national environmental trust fund website was also defaced online. All these attacks were carried out by a group of hackers calling themselves #anonymous (@Anon\_0\*03).<sup>108</sup> The insecurity scenarios raise pertinent questions whether Kenya is ready to face cyber terrorists effectively.<sup>109</sup> It must be noted that over 25 million persons have been connected to the internet in the country and thus a more improved and concerted effort is needed by the government to contain such threats. This is an analysis based on the fact that Kenya is ranked fourth in Africa in terms of the number of cyber-criminal cases recorded.<sup>110</sup>

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 or worms' attacks, Dos attack amongst others. The fraud crimes include online stealing of cash, gambling and robbery.<sup>111</sup> Cyber fraud is considered as the main source to cybercrime in Kenya and the government has categorized the crime among the highest cyber security threats. Mobile

---

<sup>106</sup> Ibid, (2017), pp. 16-19.

<sup>107</sup> Alexis, O. *SMSs used as a tool of hate in Kenya*, (2016), p. 92.

<sup>108</sup> MacAfee 2014, MacAfee Labs Threats Reports. June 2014.

<sup>109</sup> Kien, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., and Shitanda, S. Kenya CyberSecurity Report 2015. Serianu Limited, (2015), p. 89.

<sup>110</sup> Kagwanja, P. and Karanja, M. How cyber-crime complicates war on terror. *The East African*, (2014).

<sup>111</sup> Akogwu, E. *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. 67.

banking use has been named the most prone to attacks since over 1.7 trillion is transacted.<sup>112</sup>

One of the major problems in the Kenyan banking sector is that of fraud which is becoming widespread.<sup>113</sup> The increasing online and mobile banking innovations have exposed customers as well as local banking institution to emerging vulnerabilities.<sup>114</sup> 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.<sup>115</sup> Understandably, banks have been reluctant to expose such fraud, while courts are not effective in convicting the perpetrators.

### **2.3 Consequences of Cyber-Terrorism Threats**

The business environment has been changed a great deal by digital technology that has emerged in Africa.<sup>116</sup> Africa has witnessed and increased usage of internet penetration in the last decade. However, as the continent digitalize its business processes, the potential attack by cybercriminals become more complex.<sup>117</sup> In addition, the attack target weaknesses in the technology infrastructure and processes leading to huge loss of finances and valuable information.<sup>118</sup> This threat has made Africa rethink how it can better leverage the benefits derived from cyber technology use by building capacity.<sup>119</sup>

According to ITU report of 2014, the rapid growth of Information Communication Technology access in Africa has increased the Internet application as compared to countries of Asia and Latin America (ITU).<sup>120</sup> Cyberspace is an inherent part of the growth of any nation.<sup>121</sup> A robust digital system is critical for nations to advance and

---

<sup>112</sup> Wanjiku, R. Kenyan banks face challenges with secure online transactions International banks are not as successful as in other markets, (2013).

<sup>113</sup> Daily Nation (2010). Kenya: Alarm as bank employee's siphon out Sh2.4bn through "inside jobs." 10th July 2010.

<sup>114</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>115</sup> Ibid, (2017), p. 41.

<sup>116</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

<sup>117</sup> Kenya Cyber Security Report 2016.

<sup>118</sup> MacAfee 2014, MacAfee Labs Threats Reports. June 2014.

<sup>119</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), p. 119.

<sup>120</sup> MacAfee 2014, MacAfee Labs Threats Reports. June 2014.

<sup>121</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

progress in matters political, economic and social domain.<sup>122</sup> To build a stable and solid cyber capacity, there will be need to secure and utilize available Cyberspace.<sup>123</sup>

According to Burt, Nicholas, and Scoles cyber security is defined as the response to threats to an active cyberspace through the permission of persons, societies and governments.<sup>124</sup> In order to attain meaningful national development, the cyber security risks originating from access to and use of cyberspace must be minimized.<sup>125</sup> Since the beginning of 21<sup>st</sup> Century, the African continent has experienced growth in its economy and the trend seems to hold.<sup>126</sup>

The Report on Africa Economic survey of 2013, published by the Economic Commission for Africa (ECA) and the African Union Commission (AUC), pointed that Africa's growth performance had improved immensely since the beginning of the century.<sup>127</sup> The Economist<sup>128</sup> and the International Business Times<sup>129</sup> and the African Development Bank (AFDB)<sup>130</sup>, have stated that Africa is dwelling place to the world's most rapidly Growing economies.<sup>131</sup> This is portrayed in the continent's growing mid class and fast application of technology in normal activities. Further, this is explained by the number of subscribers which according to International Telecommunications Union (ITU) report of 2013 showed that the number stood at 63 percent of internet users reaching over 16 percent.<sup>132</sup>

The new Africa, as contained in the expression "Africa Rising" is mirrored in the continent's increasing acceptance of mobile technology the continent is characterized by fast development in the use and application of Information Communication Technology (ICT) both in public and private sector.<sup>133</sup> This has been enabled by the independence in the sector where both corporate and individuals compete freely in the market.

---

<sup>122</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>123</sup> Ibid, (2017), p. 35.

<sup>124</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

<sup>125</sup> Pawlak, P. *Developing capacities in cyberspace*, in Pawlak, P. (ed.) riding the digital wave: The impact of cyber capacity building on human development, (2014), pp. 9-16.

<sup>126</sup> Ibid, (2014), p. 17.

<sup>127</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>128</sup> Justine, O. *Growth and other good things*, The Economist, (2013), pp. 67-69.

<sup>129</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>130</sup> Ibid, (2017), p. 35.

<sup>131</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

<sup>132</sup> Ibid, (2019), p. 15.

<sup>133</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

According to Internet World Stats (2017), Africa has 388 million internet users showing about 10 percent penetration.<sup>134</sup> This has attracted a huge number of international investors into the continent with a view to exploit the opportunities presented by the market. Similarly, ICT Africa believes that the continent is growing to be an important technology hub in the world which is likely to fast track its growth.<sup>135</sup> Since Africa has majority youthful population of between 25-35 years who often use internet, the continent ICT penetration greatly grown compared to rest of the world.<sup>136</sup>

The ICT in Africa has presented opportunity to transform commerce and governance in driving innovations, entrepreneurship and economic growth.<sup>137</sup> The communication technology has revolutionized the internet and mobile phones uses in the continent.<sup>138</sup> The explosive development of mobile phones in the last decade shows the need for change across Africa.<sup>139</sup> With the fast penetration rate of more than half a billion mobile subscriptions in 2012, this number exceeds the figure for United States or the European Union, making Africa the second fast developing region in the world, after South Asia.<sup>140</sup> Cellular phones are widely used as a stand to facilitate access to the internet and state services because it is affordable.

According to World Bank research of between 2000 and 2008, Africa's earned an extra 1.2 percent boost to GDP which compares with other continents that have liberalized their telecom sectors.<sup>141</sup> The reason for liberalization can be attributed to the factors such as increasing political stability, higher commodity prices and reforms in most areas of the economy. As for case of Kenya mobile banking, the use of mobile phones is widely utilized in Mobile Money Transfer Services which is referred to as M-Pesa. In addition, the decision by Kenya to adopt e-government and e-commerce has opened window for

---

<sup>134</sup> MacAfee 2014, MacAfee Labs Threats Reports. June 2014.

<sup>135</sup> Ibid, (2014).

<sup>136</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>137</sup> Akogwu, E. *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. 67.

<sup>138</sup> Mutua, W. *The Significance of Mobile Web in Africa and in Future*, (2011), pp. 9-15.

<sup>139</sup> Ibid, (2011), p. 21.

<sup>140</sup> Kearney, M; Schuck, S; Burden, K and Aubusson, P. *Viewing mobile learning from a pedagogical perspective*. Res arch in Learning Technology, (2012), 1440.

<sup>141</sup> William, M., Mayer, R., and Mingos, M. *Africa's ICT Infrastructure: Building on the Mobile revolution*, World Bank, (2011), p. 91-99.



transparency and a means to fight corruption through the e-data enterprise.<sup>142</sup> Similarly, countries such as Ghana, Egypt, Nigeria and South Africa have adopted e-economy in many areas such as in Agricultural market I-tax filing sensor-based irrigation systems are some of the ICT revolutions in the continent.<sup>143</sup>

## 2.4 Mitigation Measures against Cyber Threats

Cyber terrorism can be a difficult term to define since it entails a wide spectrum of offenses many of which have already been fundamentally defined by existing law, for instance, unlawful electronic transfer of funds can be seen as fraud by already existing law and so the challenge really becomes whether to define new laws or amend existing ones.<sup>144</sup>

This section posits that it is not only within the purview of the government to fight cyber-crime but it can also be done by non-state actors who disable harmful links and sites, establish tip lines and come up with anti-malware software.<sup>145</sup> These efforts can be localized or they could have a global concerted effort since the internet has become ubiquitous in virtually all human societies.<sup>146</sup> Public awareness is critical in the fight against cyber-crime. It may even be considered the first line of defense.<sup>147</sup>

It is worth noting that even though the definition of cyber-crime may be a tricky affair, there are clearly two categories of it.<sup>148</sup> The distinction between the two categories is that with computer enabled crime is a form of crime facilitated by computer technology even though it may still have been commissioned without the support of a computer while a computer

---

<sup>142</sup> Shrekiam, E. *Cyber Crime in North Africa*, the Shape of Future Conflicts, *Journal of Crime*, (2015), p. 33.

<sup>143</sup> *Ibid*, (2015), p. 37.

<sup>144</sup> Christopher, Y. *Intelligence and Security Informatics*, IEEE ISI 2008 international workshops, (2008).

<sup>145</sup> MacAfee 2014, MacAfee Labs Threats Reports. June 2014.

<sup>146</sup> 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. 67.

<sup>147</sup> Obel, M. *Africa poised for unprecedented, long-term economic growth: Seven drivers that could transform Africa into the world's economic powerhouse*, *International Business Times*, (2013), pp. 71-79.

<sup>148</sup> *Ibid*, (2013), p. 81.

dependent crime is a crime that could not take place without use of computers and related digital technology.<sup>149</sup>

Ayantokun opines that like any other crime, cyber-crime cannot just be annihilated because there are laws on the books that exist and even vigilance from government agencies sometimes fall short of achieving their goals but what complicates the situation is the lack of a coordinated effort and coordinated law making across borders whereby laws can be harmonized so that cyber criminals do not go scot free just because where they happen to be at the time, the laws of that land have not yet criminalized an act and yet the internet is an international network.<sup>150</sup>

It is almost a rule of thumb among statisticians that the more educated a population is the less prone they will be to get involved in criminal activity. Nevertheless, many cyber criminals are well educated people and this just means that they are somehow hard wired to engage in criminal activity.<sup>151</sup> The initial step is assessment of the situation by the security agencies and trying to comprehend the technical aspects of incidents in which unauthorized access has occurred, what elements of a crime are involved in legal terms, are contained in known and objective facts.<sup>152</sup>

## **2.5 Chapter Conclusion**

Cyber-threats in Africa have developed to be prevalent and more serious to national security due to its porous nature and complexity. The increase may be due to increase in the use of computers across the public and private sectors of the economy which has attracted criminals who want to exploit the opportunities available. This section found that as shown in the trends of threats presented, the attacks have also become increasingly sophisticated because of the asymmetric nature of operations. Whereas, there are measures in place to protect the infrastructure, they are not adequate enough to cover the entire cyberspace frontage.

---

<sup>149</sup> 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).

<sup>150</sup> Ayantokun, O. *Fighting Cybercrime in Nigeria: Information-system*.www.tribune.com Ehimen, O.R. and Bola, A, (2010), Cybercrime in Nigeria. Business Intelligence Journal, January 2010, Vol.3.No.1.

<sup>151</sup> Christopher, C. *Intelligence and Security Informatics*, IEEE ISI 2008 international workshops, (2008).

<sup>152</sup>MacAfee 2014, MacAfee Labs Threats Reports. June 2014.

## CHAPTER THREE

### THE IMPLICATIONS OF CYBER TERRORISM THREAT TO NATIONAL SECURITY IN KENYA

#### 3.1 Implications of Cyber Terrorism Threats

It is generally acknowledged that there is incessant debate within the academic community as to the level at which cyber terrorism poses a possible threat to the national security system. This contestation is because of the different conceptions and definitions of cyber terrorism.<sup>153</sup>

The concept of cyber terrorism comprises illicit threats and attacks against networks, computer systems, knowledge and information contained therein by use of threats, intimidation or coercion against the state, citizens, economic, environmental political and social order.<sup>154</sup> In addition, “For any attack to be taken as cyber terrorism, ideally it should not only cause harm that generates fear in the populace, but also cause violence against persons, families, individuals, agency or property.”<sup>155</sup>

Cyber terrorism is a new addition in the security domain, with Academic literature beginning to emerge around this phenomenon.<sup>156</sup> The study of this phenomenon is dominated by three critical questions. There are four features concerning the disagreements scholars find with the term cyber terrorism.<sup>157</sup> In a broad sense, it encompasses terrorists’ online activities that include radicalization.<sup>158</sup>

In contrast, other views suggest that it should not include prior arrangements and enhance activities for offline attacks and that it should be restricted to threats that employ digital technologies.”<sup>159</sup> Second contested characteristic is the harm requirement. Scholars like

---

<sup>153</sup> Stuart, M. *Cyber terrorism: A Survey of Researchers*, Cyber terrorism Project Research Report No. 1, Swansea University, (2013), p. 3.

<sup>154</sup> Shrekiam, E. *Cyber Crime in North Africa*, the Shape of Future Conflicts, Journal of Crime, (2015), p. 37.

<sup>155</sup> Ibid, (2017), p. 14.

<sup>156</sup> The origins of the term cyber terrorism are typically located in the mid-1980s, see for example: Barry Collin, “The future of cyber terrorism”, Criminal Justice International, Vol. 13, No. 2 (1997), pp. 15-18.

<sup>157</sup> MacAfee 2014, MacAfee Labs Threats Reports. June 2014.

<sup>158</sup> Sarah, G. and Richard, F. “Cyber terrorism?” Computers and Security, Vol. 21, No. 7 (2002), pp. 636-647.

<sup>159</sup> Ibid, (2002), p. 650.

Collin describe cyber terrorism as ‘hacking with a body count.’<sup>160</sup> That is, the attack must generate physical violence against people there are counter arguments that accept significant economic.<sup>161</sup> It is worth appreciating that the third concern involves the intention or motive of the attack. Many of the existing definitions of cyber terrorism consider political or ideological motive and the creation of fear.<sup>162</sup>

Mark argues that the fourth and final issue concerns agency. Some scholars argue that only non-state actors can perpetrate such acts, while states engage in cyber warfare or cyber espionage.<sup>163</sup> However, researchers are of the view that states are also capable of engaging in cyber terrorism.<sup>164</sup> In the African perspective, particularly Kenya, cyber terrorism may overlap with traditional terrorism, cybercrime, or cyber war. However, when the attack is economically motivated than ideologically, it is considered cybercrime.<sup>165</sup> A scholar like Erbschloe in the study of information warfare explores the connection between economy and national defense.<sup>166</sup>

Weimann is of the view that cyber-attacks may be “attractive to terrorist groups because of the wider selection of cyber tools, available targets, the ability to conduct attacks remotely, and the Internet’s potential for anonymity.”<sup>167</sup> Skeptics argue that the chances of a cyber terror attack occurring are unlikely compared to the conventional terror attacks due to some of these reasons. For instance it needs a high level of technical expertise and it is costly to acquire necessary instruments.<sup>168</sup>

Wolf and Jones argue that the responses to cyber terrorism which continue to elicit considerable debate in the Kenyan context. It is acknowledged that defense-in-depth and target-hardening in which organizations use firewalls to act as a form of ‘perimeter

---

<sup>160</sup> Shrekiam, E. *Cyber Crime in North Africa*, the Shape of Future Conflicts, Journal of Crime, (2015), p. 39.

<sup>161</sup> Ibid, (2015), p. 41.

<sup>162</sup> Denning, D. *Cyber terrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Service U.S. House of Representatives*, (2018), p. 113.

<sup>163</sup> Mark, M. *Cyber terrorism: Fact or Fancy*, Computer Fraud & Security, Vol. 2 (1998), pp. 8-10.

<sup>164</sup> Heickerd, op. cit., p. 556; Lee Jarvis, Stuart Macdonald and Lella Nouri, “State Cyber terrorism: A Contradiction in Terms?” Journal of Terrorism Research, Vol. 6, No. 3 (2015), pp. 62-75.

<sup>165</sup> Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019), pp. 103-117.

<sup>166</sup> Michael Erbschloe, *Information Warfare: How to Survive Cyber Attacks* (New York: Osborne/McGraw-Hill, 2011), p. 3.

<sup>167</sup> Ibid, (2011), pp. 8-12.

<sup>168</sup> Maura Conway, “Reality Check: Assessing the (Un) Likelihood of Cyber terrorism” Springer, (2014), pp. 103-121.

defense is one frequently discussed aspect of this debate.<sup>169</sup> Development and enactment of appropriate legislation to combat cyber terrorism is an area under discussion;<sup>170</sup> however their effectiveness within the domestic environment is questionable.<sup>171</sup>

Cyber terrorism legislation faces the problems of attribution and jurisdictional scope in the cyber realm.<sup>172</sup> This difficulty is extended to states wishing to respond to cyber-attacks under international law where the acts transcend the territory of a single sovereign.<sup>173</sup> There are numerous cyber activities online that involve international commerce and finance, information sharing, and social networking media, from which a number of incidents have occurred but with varied opinions as to what constitutes a cyber-attack, an act of war in cyberspace, or cyber terrorism.<sup>174</sup> Generally, cyber war is considered as an action involving states that is equivalent to an armed attack or use of force in cyberspace that may warrant a reciprocal military attack.

Burgess states that there is ongoing debate as to whether the cyber terrorism threat is exaggerated or if its destructive and harmful effects merit concern with both the news media and government indicating that many terror groups use the net to communicate, recruit personnel, raise money and coordinate attacks.<sup>175</sup> There is no record or data showing that terrorist organizations have mounted success attacks against systems and networks, however reports indicate that many terrorist organizations have acquired capability and capacity necessary to use online means to hit their targets if the opportunity avails itself.<sup>176</sup>

Cohen and Felson argue that cyber terrorism threat requires that policy makers and security planners design and implement preemptive actions to prevent such attacks from

---

<sup>169</sup>William A. Wulf. and Anita K. Jones, "Reflections on cyber security", *Science*, Vol. 326, No. 5955 (2009), p.943

<sup>170</sup>Neal K. Katyal, "Criminal law in cyberspace", *University of Pennsylvania Law Review*, Vol. 149, No. 4 (2001), pp. 1003-1114; Richard W. Downing, "Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime", *Columbia Journal of Transnational Law*, Vol. 43, No. 3 (2005), pp. 705-762.

<sup>171</sup>Patrick Bishop, "Cyber terrorism, Criminal Law and Punishment-based Deterrence" in T. Chen, L. Jarvis and S. Macdonald (eds.), (Abingdon: Routledge, 2015), pp. 107-124.

<sup>172</sup>Hug and Bapna, *op. cit.*, pp. 102-114.

<sup>173</sup>Susan W. Brenner, "Cybercrime jurisdiction", *Crime, Law and Social Change*, Vol. 46, No. 4-5 (2006), p.190.

<sup>174</sup>Burgess, Matt. What is GDPR? WIRED explains what you need to know. *Wired*, (2018), p. 12-19.

<sup>175</sup> *Ibid*, (2018), p. 21.

<sup>176</sup>Brenner, W. *Cybercrime: Criminal Threats from Cyber Space*. Santa Barbara, California: Greenwood Publishing Group, (2010), p. 38.

occurring.<sup>177</sup> Translating this theory to cyber technology, shows that the ICT evolution is not without challenges. The advancing nature and falling costs of ICT has given rise to digitalization of economies in Africa.<sup>178</sup> The internet has fundamentally transformed the continents political, economic and social lives.

Brenner contends that cyber threats were first heard in 1990s in Africa. This is the period that internet and private computers began to be sophisticated and universal.<sup>179</sup> Since the improvement of technology and the advent of the internet gave rise to cybercrime, it has been understood as a crime that takes place precisely over networks.<sup>180</sup> Cybercrime is ranked amongst the top threats to national security in the world.<sup>181</sup>

The Symantec report of 2016 indicates that the number of targeted cyber-attacks in Africa grew by 42 percent.<sup>182</sup> Of concern, 31 percent were categorized as cyber espionage targeting governments and business enterprises. Nigeria was found to be the most affected country with the main source being malicious internet activities which has also affected other nations in the West African sub-region.<sup>183</sup> Similarly, major cities in the continent which are well served with Information Technology have experienced cyber-attacks especially in industries, security and financial sectors.<sup>184</sup>

### **3.2 Cyber Terrorism on Critical Infrastructure in Kenya**

Cyber terrorism merges two spheres, terrorism and technology; critical concepts that require comprehensive counter strategies that are more proactive rather than reactive. To help in understanding and determining effective strategies and the thinking behind them, theoretical considerations are addressed.<sup>185</sup> This involves an analysis of deterrence theory and its consequent effect on cyber terrorism.

---

<sup>177</sup>Cohen, L and Felson, M. Social change and crime rate trends: A routine activity approach, *American Sociological Review*, (1997), pp. 588-589.

<sup>178</sup>David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>179</sup>Brenner, W. *Cybercrime: Criminal Threats from Cyber Space*. Santa Barbara, California: Greenwood Publishing Group, (2010), p. 38.

<sup>180</sup>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,

<sup>181</sup>Gercke, M. The Slow Wake of a Global Approach against Cybercrime, *Computer Law Review International*, (2006), p. 89.

<sup>182</sup> Ibid, (2012), p. 126.

<sup>183</sup> 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), p. 161.

<sup>184</sup> Gady. F.S. *Africa Cyber world*. (2010), p. 35.

<sup>185</sup> Ibid, (2010), pp. 37-41.

Critical infrastructure requires protection against terrorist attacks. This is because such infrastructure may have vulnerabilities that can be exploited by terrorist.<sup>186</sup> Each state has the obligation to identify what constitutes its critical infrastructure. Schulman and Roe define critical infrastructure as the “basic capabilities, technical systems and organizations which are responsible for the provision of assets”<sup>187</sup> The European Commission defines critical infrastructure as an “asset or system which is essential for the maintenance of vital societal functions”<sup>188</sup> Critical Infrastructure is defined as “systems and assets, whether physical or virtual, vital to the state such that the incapacity or destruction of such systems and assets would have a debilitating impact on the security, national economic security, safety, or any combination of those matters.”<sup>189</sup>

Kenya enacted a law on cyber security “Information and Communications Act 2009, according to this report, the legislations are not adequate to address the challenges of computer crimes”.<sup>190</sup> The country lacked sufficient legislative policy and administrative framework to compel institutions as well as individuals to secure and protect personal data.<sup>191</sup> In realizing the wide and dynamic nature of ICT challenges, Kenya has developed strategies to guide cyber security at the national level to enable economic growth and protect the interests of the people.<sup>192</sup>

The Kenya National Cyber Security Master Plan is a strategy document that has been developed to address the risks that ICT may face in the future. The Strategy is based on the three pillars of Vision 2030 which define Kenya’s cyber security and objectives to be

---

<sup>186</sup> CTED Trends Report (2017), Physical Protection of Critical Infrastructure against Terrorist Attacks

<sup>187</sup> Schulman, P.R., and Roe, E. (2007) Designing Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures. *Journal of Contingencies and Crisis Management* Volume 15 Number 1 March 2007.

<sup>188</sup> Leverett, Eireann. *Cyber Terrorism: Assessment of the Threat to Insurance*, Cambridge Risk Framework series: Centre for Risk Studies, University of Cambridge, (2017), p. 12-13.

<sup>189</sup> IHS Janes “Adopting a holistic approach to Protecting Critical Infrastructure (2014).

<sup>190</sup> Ibid, (2009), p. 163.

<sup>191</sup> Constitutional implementation in Kenya, 2010-2015: Challenges and prospects, FES Kenya Occasional Paper, No. 5 ISBN: 9966-957-20-0.

<sup>192</sup> The East African, Kenya Launches Centre to fight cybercrime, (2016).

achieved in order to secure a safe cyberspace.<sup>193</sup> This has been achieved by enacting Kenya Information and Communications ACT, CAP 411A which is an amendment to ICT ACT, 2014 and establishes a National Certification Authority Framework, which is intended to provide a foundation for public key partnership with regional and international cybersecurity bodies. This includes forums such as ITU and East Africa Communications Organization (EACO).<sup>194</sup> 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.<sup>195</sup>

### **3.3 Emerging Patterns of Cyber Technology as a National Security Threat in Kenya**

The cyber threats of sexting have posed an especially difficult problem for enforcers of the law in Kenya. In this crime sexually suggestive and semi-or fully nude pictures are disseminated through networks accessed through internet from cellular devices like smart phones and iPad or even laptops.<sup>196</sup> There are many studies that have attempted to explain why sexting has been a popular activity to engage in by youths.<sup>197</sup> This Conrad found that Communication Authority has been leading campaigns to sensitize families on the issue of cybercrime including ethical hacking pathways while at the same time remaining cautious of the negative effects it could have like scaring off the youth's talents in all areas of application of Information Technology.<sup>198</sup>

The involvement of both parents and children in understanding cybercrime and activities such as such as hacking is critically important. When minors break the window of a shop, one can clearly understand it as a crime they have committed.<sup>199</sup> But for when the minors are

---

<sup>193</sup> Leverett, E. *Cyber Terrorism: Assessment of the Threat to Insurance, Cambridge Risk Framework series: Centre for Risk Studies*, University of Cambridge, (2017), p. 12-13.

<sup>194</sup> Gagliardone, I., and Sambuli, N. *Cyber Security and Cyber Resilience in East Africa*. Centre for International Governance Innovation, (2015), pp. 8-12.

<sup>195</sup> Fischer, E. *Creating a National Framework for Cyber security: An Analysis of Issues and Options*, February 22, CRS Report for Congress, Order Code, (2005), pp. 7-9.

<sup>196</sup> Conrad, J. *Seeking help: the important role of ethical hackers*. Network Security, (2012), pp. 5-8.

<sup>197</sup> Ibid, (2012), p. 10.

<sup>198</sup> 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), p. 169.

<sup>199</sup> Leverett, Eireann. *Cyber Terrorism: Assessment of the Threat to Insurance, Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge*, (2017), p. 12-13.



exploring the internet or “surfing” as they sometimes refer to it, their behavior online in the form of hacking may remain unclear.<sup>200</sup>

It is therefore imperative for more precise education and instructions to be formulated and to include clear detailed definitions, information about what kind of harm such behavior is capable of causing on victims and the legal implications and consequences to the perpetrators of such behavior. Cyberspace security is a big and important issue for the state and non-state actors. More and more of everyday life activities and transactions are now done online including banking, tax transactions, health care and even monitoring of residence.<sup>201</sup> This implies the need for enormous investments in cyber security to protect the stored and transmitted data from a potential attacker.

Cyber mercenaries can be defined as “anyone with an online presence who is willing to sell their expertise to interested third party who is willing to pay to acquire digital access to high profile networks or victims.”<sup>202</sup> Cyberspace is the term is simply used to refer to the network which is known by most people as the internet. By definition cyberspace is more than the internet. Internet is just one of the divisions within cyberspace to which this section focused. Internet has also developed further from the traditional WWW on which it was based and now has capabilities for audio and video streams or data, complex gaming and can allow one to switch between multiple websites.<sup>203</sup>

Kenya and Tanzania have been the biggest sufferers due their lead in use of technology and electronic financial application. The countries have reacted by enacting laws that counter cybercrime.<sup>204</sup> The regulations seem to be having gaps which are still being exploited by criminals. Law enforcers also lack the necessary capacity in terms of equipment and training to handle cybercrime.

---

<sup>200</sup>William A. Wulf. and Anita K. Jones, “Reflections on cybersecurity”, *Science*, Vol. 326, No. 5955 (2009), p. 943.

<sup>201</sup> *Ibid*, (2009), 945.

<sup>202</sup> Brenner, W. *Cybercrime: Criminal Threats from Cyber Space*. Santa Barbara, California: Greenwood Publishing Group, (2010), p. 38.

<sup>203</sup> Leverett, Eireann. *Cyber Terrorism. Assessment of the Threat to Insurance*, Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge, (2017), p. 12-13.

<sup>204</sup> *Ibid*, (2017), p. 12-13.

Anonymous features on the cyber space have both a positive and negative impact on how the internet affects people's lives.<sup>205</sup> Such features enable people to have freedom of expression especially in oppressive societies, give them the ability to have freedom of information, privacy and communication but this feature is a double edged sword as it leads to cyber criminals being able to do their bidding while being untraceable. Some of these criminal activities may involve cyber stalking, opening up child porn sites, intimidation and bullying and many more.<sup>206</sup>

Cybercrime in Kenya is on the rise it is estimated to cost over United States Dollars (USD) 175 million and the cost continues to rise as long as many organizations automate their service processes.<sup>207</sup> This is particularly the case since financial institutions continue to 'introduce mobile and e-services which has led to new weaknesses in the system resulting to losses of funds.<sup>208</sup> The E-commerce for instance has been susceptible serious online scams such as Automatic Teller Machine card skimming and identity theft by unsuspecting cybercriminals. Similarly, electronic banking and cashless services that have been introduced into the country have further complicated the situation.<sup>209</sup>

Kenya, in Africa is a leading target in online money fraud due to its advanced mobile money market. It has been estimated that about 30 billion US dollars are transacted via mobile money every year in Kenya alone and this has painted a huge bull's eye, so to speak, on the country for cyber criminals.<sup>210</sup> In recent past Kenyan banks ranged from insider threats to spear phishing and ransom ware attacks. Banks are vulnerable through their vulnerable web applications, Internet and Mobile banking platforms which have attracted cybercriminals.

Kenya has experienced numerous mobile money threats, resulting through malware attacks and personifications of account. As banks embrace e-finance services, hackers are busy

---

<sup>205</sup>William A. Wulf. and Anita K. Jones, "Reflections on cybersecurity", *Science*, Vol. 326, No. 5955 (2009), p.943

<sup>206</sup> Leverett, Eireann. *Cyber Terrorism. Assessment of the Threat to Insurance*, Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge, (2017), p. 12-13.

<sup>207</sup> *Ibid*, (2017), p. 17.

<sup>208</sup> Fischer. Eric. *Creating a National Framework for Cyber security: An Analysis of Issues and Options*, February 22, CRS Report for Congress, Order Code, (2005), pp. 11-21.

<sup>209</sup> Maina, Charles. *A survey on impact of ICT on Business Value Creation in Kenya Banking Sector*. Unpublished MBA project, University of Nairobi, (2010), pp. 9-13.

<sup>210</sup> Brenner, W. *Cybercrime: Criminal Threats from Cyber Space*. Santa Barbara, California: Greenwood Publishing Group, (2010), p. 38.

fighting to exploit weaknesses immobile money security controls with an aim to steal.<sup>211</sup> Malwares presents in several forms such as Trojans worm called Dridex and Zeus malware which are very effective. These types of malwares are known to compromise targets making them easy to access sensitive information on the network.<sup>212</sup>

### **3.4 Kenya Cyber Security Measures and Strategies**

Kenya has ambitiously emerged as EAC leading ICT manager in the region and has made great progress in integrating ICTs 'into most sectors of the industry. The ICT sector has experienced extraordinary growth in the last decade in the area of socioeconomic development.<sup>213</sup> 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 in order to achieve Vision 2030.<sup>214</sup> The ICT infrastructure has been included in public policy as a tool to improve the livelihood of Kenyans through provision of affordable services.

The Internet was first introduced to Kenya in 1993 and full usage was established in 1995. The first internet ISP Form net commercial application became operational in 1995 and many more ISPs have joined the broadband market which has been transformed through increased investments in digital network.<sup>215</sup> The expansion has enhanced broadband services which have been made affordable for the market. In 2000, Kenya had about "200,000 Internet users with an assessed monthly growth of 300 new subscribers.<sup>216</sup> The mobile penetration has increased from 89.2 percent to 90 percent according to the CAK Report.<sup>217</sup> The sustained growth in subscriptions of mobile phones has been enhanced by proliferation of affordable handsets and mobile data services including banking and commerce.<sup>218</sup>

---

<sup>211</sup> Leverett, Eireann. Cyber Terrorism. Assessment of the Threat to Insurance, Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge, (2017), p. 12-13.

<sup>212</sup> Ibid, (2005), p. 23.

<sup>213</sup> William A. Wulf. and Anita K. Jones, "Reflections on cybersecurity", Science, Vol. 326, No. 5955 (2009), p.943

<sup>214</sup> Kenya Vision 2030, (vision2030@kenya.go.ke)

<sup>215</sup> Communications Authority of Kenya. First quarter sector statistics report for the financial year 2015/2016.

<sup>216</sup> Ibid, (2016).

<sup>217</sup> David Souter and Monica Kerretts-Makau, "Internet Governance in Kenya: An Assessment for the Internet society, 'Internet society, (2012).

<sup>218</sup> Communications Authority of Kenya, Quarterly Sector Statistics Report: Q2 of the Financial Year 2016/2017.

### **3.5 Chapter Summary**

This section argues that despite these efforts, the country has faced one of the major international cybercrime cases which have exposed existing cyber weaknesses and gaps in the infrastructure. In December 2014, the country witnessed intrusion into its cyberspace by a number of foreigners from Thailand and China nationals who were arrested in Nairobi and found in possession of equipment believed were to be used for hacking into ICT networks.

The group intended to hack into Safaricom M-Pesa (mobile money transfer) system, bank accounts including Banks Automatic Teller Machines. Kenya is considered risky as a major information security hotspot in the world because of lack of awareness on the threats posed to the internet users. The absence of a devoted cyber security regulatory and legal framework places the country at a crossroad. The phenomenon of computer associated cyber terrorism is well known in the country and the increasing global connectivity is likely to have serious consequences.

## CHAPTER FOUR

### STRATEGIES TO COUNTER CYBER TERRORISM IN KENYA

#### 4.1 Research Findings

This chapter analyzes the findings, interpretations and presentations of field data aligning with the strategies and measures employed to counter cyber terrorism in Kenya. The collection of data was done through an interview guide, sorted and analysed. Content analysis and document analysis techniques were chosen as a method for data analysis.

The final outcomes of the research were presented by way of narratives, bar graphs, frequency tables and pie charts. Each respondent and their subsequent contributions were then represented by an alphabet and later analyzed through EvIEWS<sup>219</sup> software version 10 (EvIEWS ten offers academic researchers, corporations, government agencies, and students' access to powerful statistical).

The target population for this study included key stakeholders from the Ministry of Foreign Affairs, Kenya Information Communication Technology Authority, Information Communication Technology, Kenya Defense Forces, National Police Services, National Counter Terrorism Center, Immigration Department, Kenya Prison Service, Kenya Civil Aviation, National Intelligence Service and Parliament.

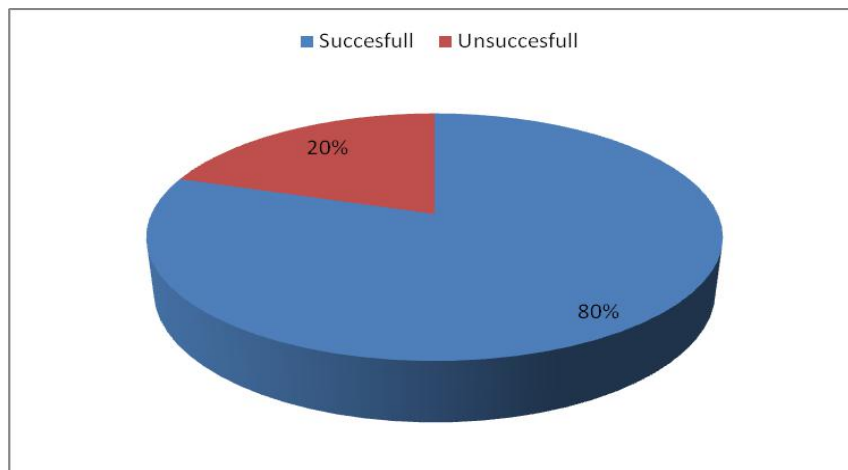
This study found 35 out of the targeted 50 respondents successfully filled the interview guide thus the 80 percent response rate. The return rate by the respondents was above 70 percent which was adequate as Borg and Gall put it.<sup>220</sup> The respondents were coded in alphabetical order A – QQ to protect their identity; hence each respondent and their subsequent contributions were represented by an alphabet.

---

<sup>219</sup> Brenner, W. *Cybercrime: Criminal Threats from Cyber Space*. Santa Barbara, California: Greenwood Publishing Group, (2010), p. 38.

<sup>220</sup> Borg, R. and Gall, D. *Education Research. 6<sup>th</sup> Edition*. New York Longman Inc (1996), p. 17.

Figure 1: The return rate



Source: Field Data (2020)

This figure 1 shows the study successfully interviewed 80 percent of the respondents. This response rate was possible as a result of actively pursuing the respondents, proper orientation of the them in to the study, accessibility of many respondents at the time of the study, the ability of the researcher to effectively apply proper research technique in the study and finally because of proper guidance from the supervisor.

#### 4.1.1 Personal Profile

This section gave the general profile of the research findings.

##### 4.1.1.1 Age distribution

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

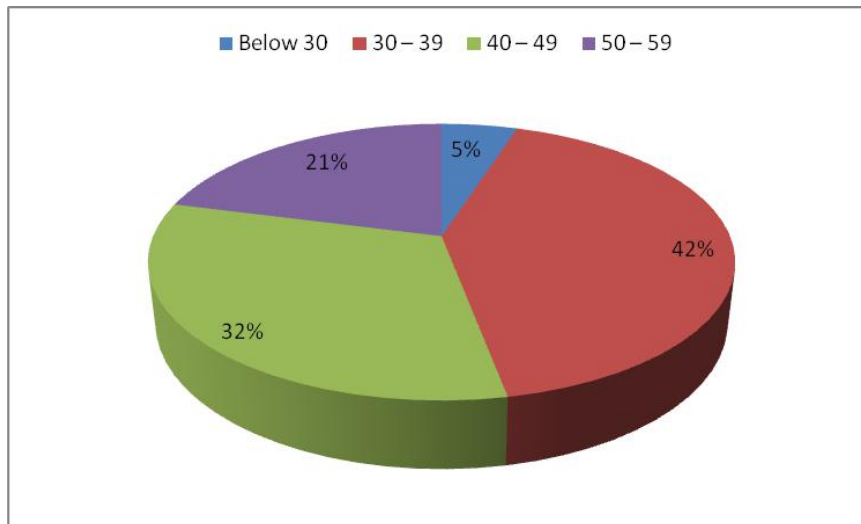
Table 1: Age of Respondents

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

Source: Field Data (2020)

The results as presented in table 1 below show the distribution is higher among the younger respondents aged 30 - 39 years, followed closely by the middle aged group of 40-49 years.

Figure 2: Age distribution



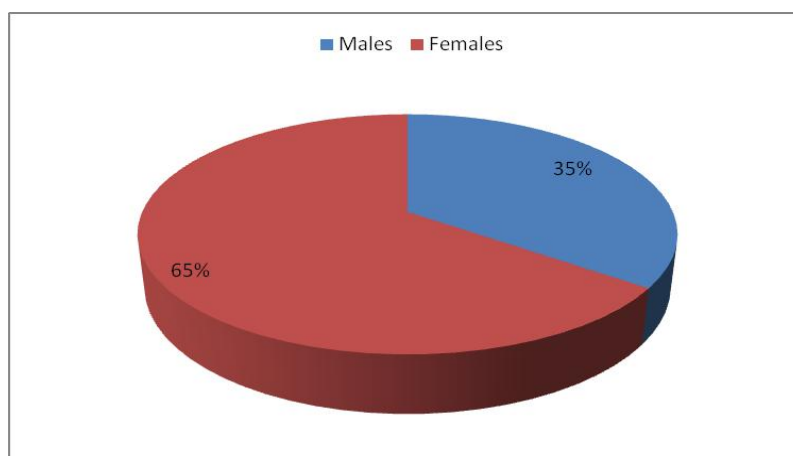
Source: Field Data (2020)

This figure 2 shows the age distribution of the respondents, an indication that the mostly young people are the most exposed to cyber related activities.

#### 4.1.1.2 Gender distribution

The 50 respondents were to indicate which gender they are and from the 35 who responded and as in the results in figure 3, that is, 25 (65 percent) were male and 13 (35 percent) were female.

Figure 3: Gender of respondents



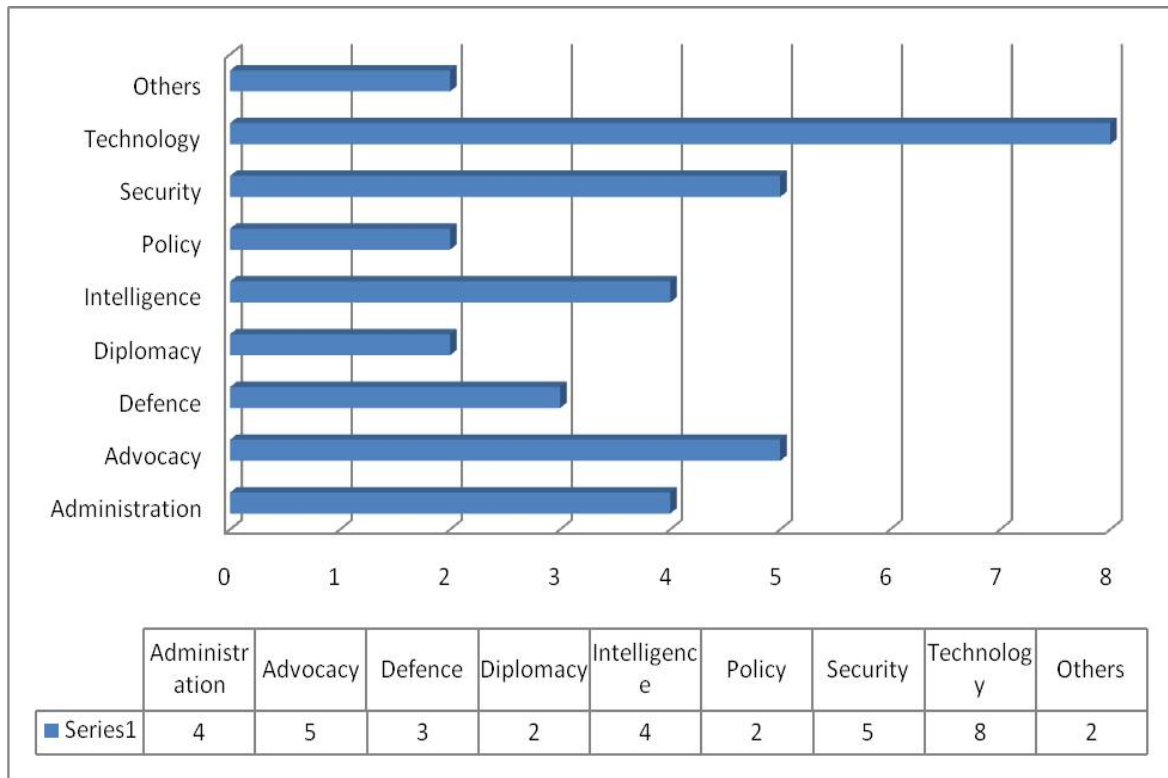
Source: Field Data (2020)

This Figure 3 shows the gender distribution of the respondents, the number of males that responded was higher than that for female. Even with the Kenyan gender rule factor is constant, more male professionals are involved with Information Communication Technology sector directly and are therefore more likely to be affected by or involved in cybercrime.

### 4.1.1.3 Occupation Distribution

The respondents were requested to indicate their occupation of origin.

Figure 4: Distribution by occupation office



Source: Field Data (2020)

The Figure 4 shows that when it comes to the cyber technology and insecurity in Africa (Kenya), the most directly affected occupation were those from the technology sector (8) and the security sector (5), and advocacy (5) respectively



#### 4.1.1.4 Designation

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

Table 2: Designation of Respondents

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

Source: Field Data (2020)

The results as presented in Table 2 show the distribution is terms of designation, highest being managers (28 percent) and indication that they are designation that most interacts with cyber issues.

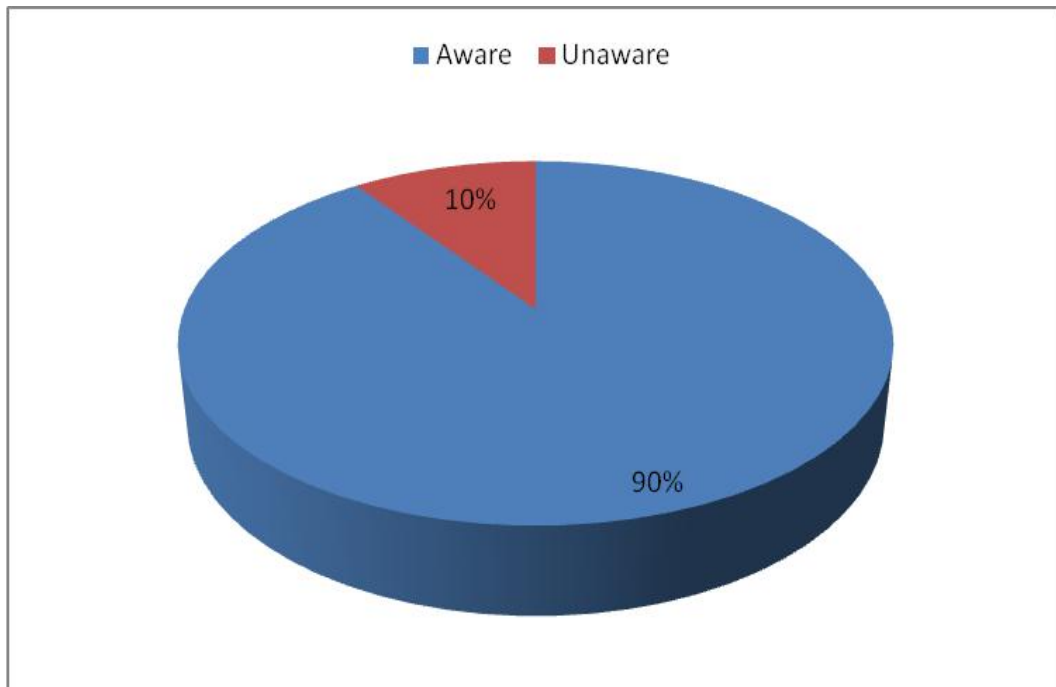
#### 4.1.1.5 Duration in Office

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

#### 4.1.1.6 Concept of Cyber Terrorism

In seeking to search for the cyber terrorism, the targeted respondents were to respond on whether they were aware of the cyber threat concept. The results were that that 90 percent were aware of it as a concept and they had at least experienced it in their line of duty. Only 10 percent were fully unaware of it as they could not define it accurately.

Figure 5: Awareness of cyber threat concepts



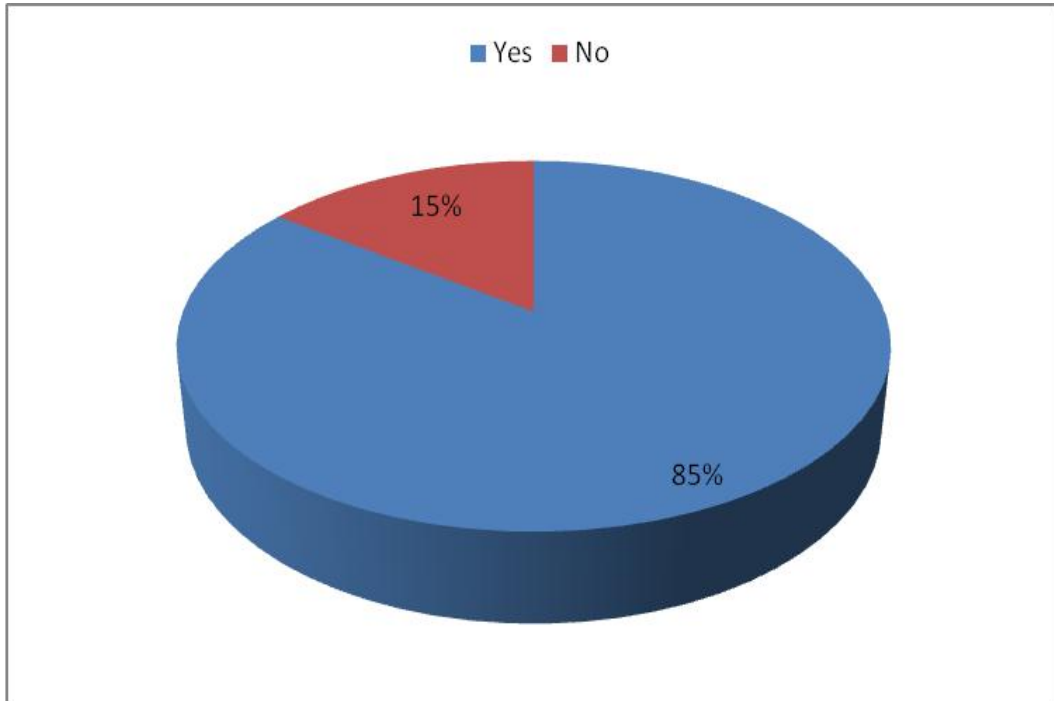
Source: Field Data (2020)

The respondents were asked of their awareness of the concept of cyber terrorism, the responses are presented in Figure 5.

#### 4.1.1.7 Witnessed any Form of Cyber Terrorism

In search for the cyber terrorism and national security in Africa using the case study of Kenya, the targeted respondents were to respond on whether they had experienced (witness) cyber terrorism.

Figure 6: Cyber attacks witness



Source: Field Data (2020)

The Figure 6 shows that 85 percent had witnessed or experienced cyber attacks in their line of duty 15 percent stated that they had not yet witness cyber terrorism.

## 4.2 Cyber Threat and National Security

This study aimed to determine the cyber terrorism and national insecurity as shown in (Figure 6).

### 4.2.1 Prevalence of Cyber Technology Threats in Africa

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

Table 3: Prevalence of cyber threat

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

Source: Field Data (2020)

This shows that that majority of the cyber attacks was cyber fraud (23%), phishing (17%) and the evidence of the research data are interlinked with the findings of the study as shown in Table 3.

This section aimed to identify the prevalent type of cyber attack they most experienced in the respondents respective organization(s) The findings on Table 3 were in agreement with the similar PWC (2015) that showed that in today's unstable economic environment, the opportunity and motivations to commit frauds have been on the rise.

In addition the (Table 3) concurred with the revelations of Mallory, (2017),<sup>221</sup> who stated that cyber threats and cybercrime are a crime associated with internet technology which concerns citizens, governments and industries where crime manifests in the form of either cyber stalking, phreaking (arching to obtain free telephone calls), piracy, cyber terrorism and cyber

---

<sup>221</sup> Mallory S, L. (2017). *Understanding Organized Crime*, Jones and Bartlett, pp. 91-99.

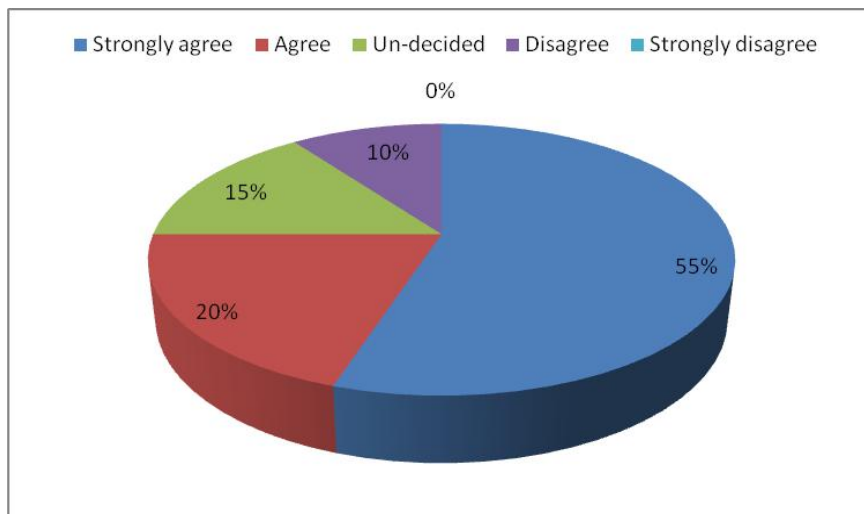
pornography. In view of this understanding, it is therefore possible to argue that all stages of computer use are vulnerable to criminal activity either as a key target or agent of cyber fraud.

Finally, this study notes that based on the data (Table 3) this research infers that cyber attacks are on increase as shown by the number of very many cases identified and experienced in various organizations as illustrated by Figure 4. This therefore confirms that a wide array of threats to national security exists as a whole and perpetuated by cybercriminals as pointed out by a respondent who stated that most of those involved with cybercrimes are youths who have found an easy way of live by hacking into organization accounts to gain information or money. In addition, this chapter notes that the majority of ICT managers are between the ages of 30-49 years who account for 80 percent as shown in (Table 1), yet cybercrime perpetrators are youths, which clearly points to a disconnect between the vulnerable youths and the ICT policy makers.

#### 4.2.2 Cyber insecurity has a direct influence on a Country’s national security

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

Figure 7: Cyber insecurity and national security



Source: Field Data (2020)

The outcome from a population of 35 the main respondents revealed that, strongly agree (55%), Agree (20%), Undecided (15%) and finally Disagree (10%). This research findings were confirmed by Internet Security Threat Report (2013), that revealed that cyber threats is an increasing global phenomenon<sup>222</sup>, the crime is increasing at a faster rate in Africa than in any part of the world. Most experts approximate that 80 per cent of individual computers on

<sup>222</sup>Symantec Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18 (April, 2013).

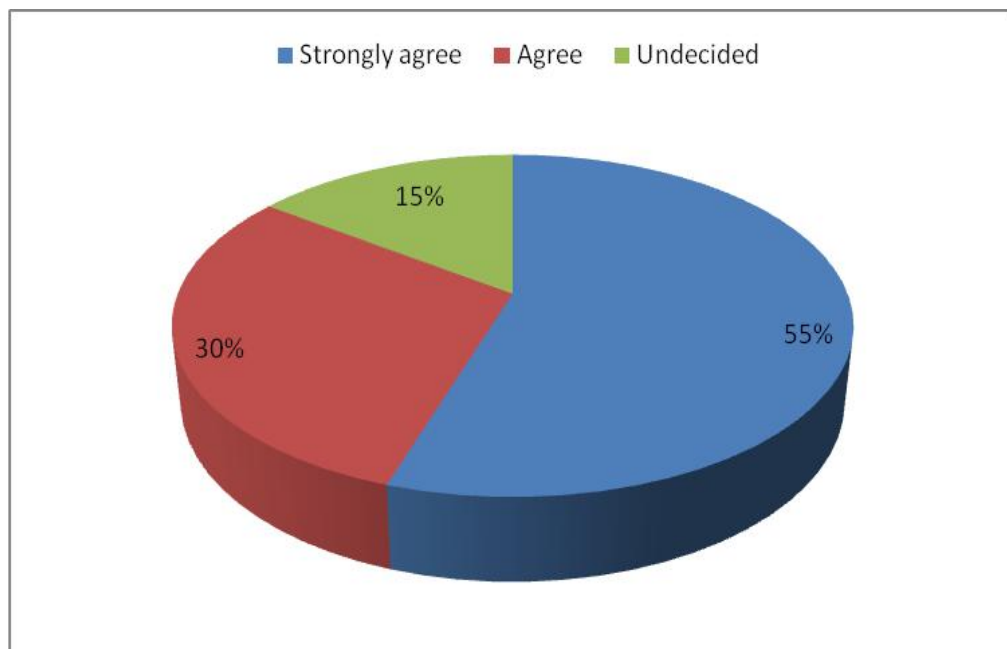
the African continent are infected with viruses together with other malicious software, (Ranz-Stefan Gacy, 2010).<sup>223</sup>

The cyber threats rate in Africa associated with digital use especially in the social media and the face book which is the highly visited website has been identified as the most popular crime zone. The youth are usually the champions of innovation, while policy makers are bureaucratic. The major crimes perpetuated include cyber bullying hate speech in form of short text messages, hacking, phishing and many others are a serious threat to national security. This thus aligns with the results findings in (Table 3).

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

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

Figure 8: Incidences of Cyber threats



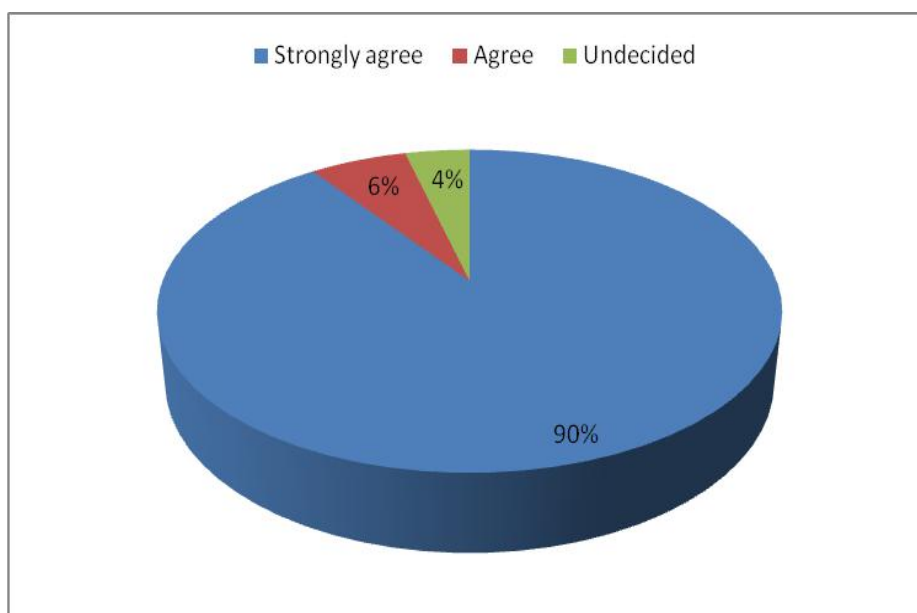
The figure 8 shows the outcome from a population of 35 participants showed that, strongly agree (55%), Agree (30%), and Undecided (15%).

#### 4.2.4 Current economic challenge has been used to justify cyber threats

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

<sup>223</sup>Ranz-Stefan Gacy, "Foreign policy: Africa's internet threat", National Public Radio, (29 March 2010).

Figure 9: Justifications for cyber threats



Source: Field Data (2020)

The Figure 9 results are in agreement with Siegel, *et al.*, who state that most common types of computer fraud include computer operations where intangible assets represented in data such as money transactions are lucrative targets of fraud related to computer.<sup>224</sup>

Based on these findings (Figure 7, Figure 8 and Figure 9), this section infers that the reliance on internet penetration and technological advancement, exposes Africa to cyber security threats, for instance Kenya for has witnessed increased cyber-attacks targeting both private and public sectors. Clearly as shown in (Table 3), as proved by the fact that the Country is highly dependent on the internet to transact major businesses it thus stands the risks of attacks as confirmed from these findings. In addition, the study infers that Kenya currently experiences growing cyber frauds involving mobile banking.<sup>225</sup> Since most users have little knowledge on cyber security, they are most likely to fall victims of internet frauds.

<sup>224</sup>David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>225</sup> Ibid, (2017), pp. 41-44.

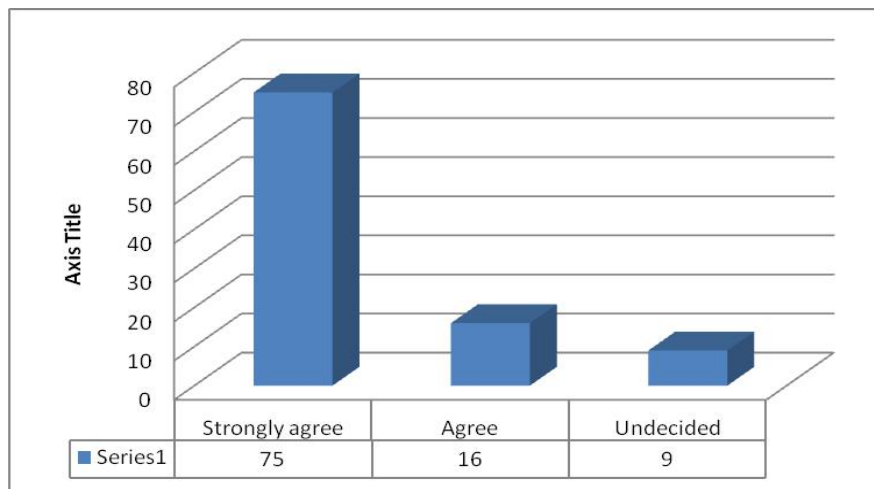
### 4.3 The emergent patterns of cyber terrorism as a national security threat in Kenya

This section gave a brief summary of the patterns and trends of cyber terrorism.

#### 4.3.1 Patterns of cyber technology threats

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

Figure 10: Increase in pattern of cyber threats



Source: Field Data (2020)

This section infers, based on (Figure 10), which the threats of cyber-attacks have greatly increased with development in information technologies which are complex in nature. Cyber threats have been known to have serious consequences to most societies, especially when they are used to coordinate attacks directed at key national infrastructures. The (Figure 10) findings were reinforced by Kenya Cyber Security Report, (2016) which indicates that Kenya has been among the major consumers of information technologies.



#### **4.4 Counter cyber security measures and strategies applied in Kenya**

The study sought to find out awareness of the existence of Cyber Security Policy in Kenya.

##### **4.4.1 Knowledge on cyber security policies, strategies and legal framework**

The majority of the respondents agreed that there exists Policies and Strategies on Cyber Security which provide guidance on cyber security and safety measures. A total of 60 percent strongly agreed that Cyber Security Policy has helped in mitigating cyber-attacks, 20 percent agreed while 10 percent were not aware. About 15 percent were able to identify Cyber Security Policy and Strategy of 2014 and 70 percent not able to precisely name any policy while 20 percent were not sure.

On the basis of these findings (Section 4.4.1) above, Kenya has policies and strategies to contain cyber threats. In addition most African states have equally adopted different frameworks to contain the threats peculiar to their environment.<sup>226</sup> Most African States such as Kenya, Uganda, Cameroon and Botswana have started to enact cyber legislations and establish sub-regional collaboration instruments to combat cybercrime. Senegal and Morocco are contemplating on joining the AU Convention. On the other hand, West African nations of ECOWAS are considering to adopt the “Commonwealth Model Law on Computer Related Crime and the Council of Europe’s the Budapest Convention on Cybercrime and Directive on Fighting Cybercrime”.<sup>227</sup>

---

<sup>226</sup> Schell, B. H. and Clemens, M. *Cybercrime: A Reference Handbook*, ABCCLIO, (2004), p. 9.

<sup>227</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

#### 4.4.2 The cyber security measures in Kenya

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

Table 4: Cyber security measures in Kenya

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

Source: Field Data (2020)

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

The findings in (Table 4) are similar to those made in Cyber Defence East Africa 2017 Conference, which discussed the different measures taken by Kenya, which included the necessary institutions and legal framework addressing cyber threats facing the country.<sup>228</sup> The strategies include the involvement of international organizations, national institutions and stakeholders. The measures include developing cyber capacity and national institutions to provide a secure and safe cyber environment. Among the achievements is the development of the Kenya National Cyber Security Master Plan 2017/18, response centres and enacted laws to secure the ICT infrastructure against emerging threats.

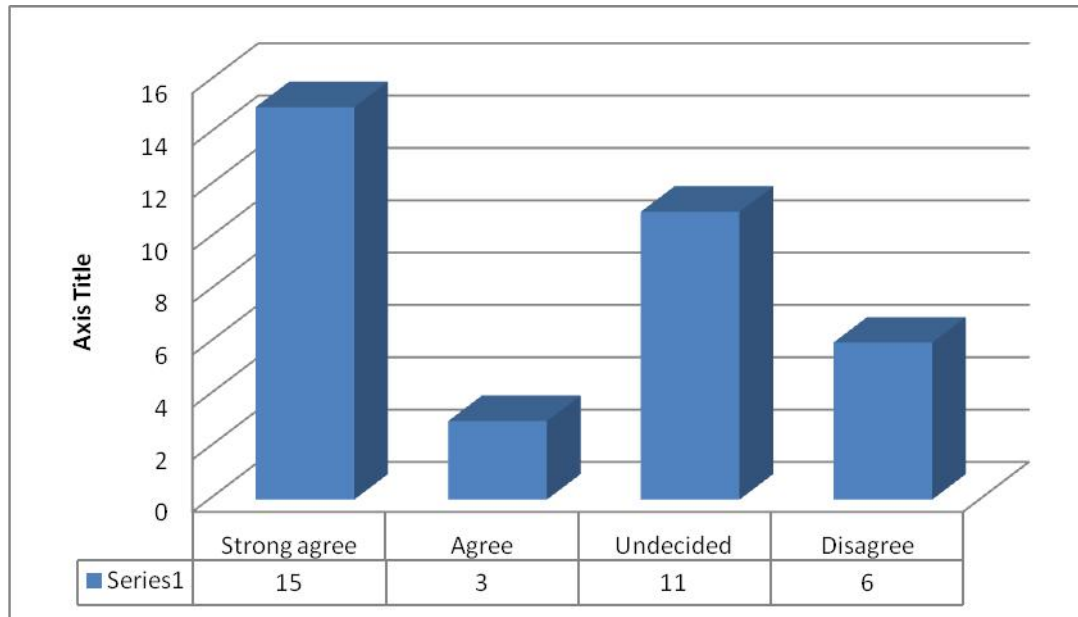
---

<sup>228</sup> Cyber Defence East Africa 2017 Conference, August 2017 Kampala, Uganda, (2017).

### 4.2.3 Achievements in the fight against cyber threats

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

Figure 11: Achievements in the fight against cyber threats



Source: Field Data (2020)

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

This research finding were confirmed by who found that Kenya, through the Communication Authority of Kenya had established a consumer awareness programme as a component of national cyber security initiative and so far the initiative had been successful in thwarting cyber threats. The East Africa Community (EAC) states have also followed the example and are on discussions to establish a cyber-science centre of excellence.<sup>229</sup>

On the other hand, the respondents who were undecided (Figure 11) stated that the vulnerabilities of Kenya's cyber space to attacks is due to the growing digitalization without a corresponding defence capabilities. The degree of cyber risks is directly linked to the degree of growth in global digitalization. These sentiments were echoed by Serianu Consultants in

<sup>229</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

Cyber Security (2015)<sup>230</sup> who stated that the institutions dealing with cyber security are not keeping in pace with the rate in which digital technologies are developing.

The respondents (Figure 11) who were undecided on whether there were achievements in the fight against cyber threats, states that, despite these efforts, the country has faced one of the major international cybercrime case which has exposed existing cyber weaknesses and gaps in the infrastructure. This outcome (Figure 11) seem to correspond to the fact that in December 2014, the country witnessed intrusion into its cyberspace by a number of foreigners from Thailand and China nationals who were arrested in Nairobi and found in possession of equipment believed were to be used for hacking into ICT networks. The group intended to hack into Safaricom M-Pesa (mobile money transfer) system, bank accounts including Banks Automatic Teller Machines (ATM) (Agence France-Presse 2014), (Otuki 2014).<sup>231</sup> According to the Kenya Police, the suspects were charged with the offence of operating telecommunication facility which was not licensed (Daily Nation, 2015).<sup>232</sup>

In addition this section aimed to further expound on the approaches to counter cyber security measures and strategies advanced in Kenya, as shown in (Figure 5, 8, 9, 10 and 11). Whereas the Country continues to lead in mobile money usage across Africa, with this growth, comes a whole new set of cyber threats; mobile malware, third-party apps, unsecured Wi-Fi, risky consumer behavior among others as outlined in Table 3.<sup>233</sup> Therefore whether or not an institution uses proprietary or third party mobile applications, pose risks to the systems which are still inherent.

In addition (Figure 10 and 11) was recently supported by the fact that The Kenya Revenue Authority (KRA) sued internet giant Google following a mystery hacking of the taxman's systems. Hackers breached the Kenya Revenue Authority's systems, prompting an investigation. KRA detectives are engaged in a landmark court battle with Google over access to an email at the centre of the hacking. The Directorate of Criminal Investigations has

---

<sup>230</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

<sup>231</sup> Ibid, (2017), p. 37.

<sup>232</sup> Daily Nation. 2015. "Try Crime Suspects Here." Daily Nation, January 15. [www.nation.co.ke/oped/Editorial/ChinaKenya-Hacking-Trial/-/440804/2590722/-/fcv6r1z/-/index.html](http://www.nation.co.ke/oped/Editorial/ChinaKenya-Hacking-Trial/-/440804/2590722/-/fcv6r1z/-/index.html).

<sup>233</sup> Wasuna, Brian. *Taxman, google Kenya in court battle over mystery KRA hack*. The Star Newspaper, Nairobi, Kenya, (2018), p. 12.

obtained a court order granting it access to an email address used by the hacker.<sup>234</sup> KRA has served the order to Google's local subsidiary, but the American firm says it is not in a position to assist in the probe. KRA is in a separate court case in which it wants to recover Sh4 billion from another suspected hacker, Alex Mutuku. This person had previously been accused of hacking into Safaricom and NIC Bank systems. His case with the KRA is still pending at the High Court.<sup>235</sup>

The (Figure 10 and 11) is corroborated by the fact that in the month of February 2018, financial institutions suffered major cyber attack and this confirms that attacks targeting Kenyan banks ranged from insider threats to spear phishing and ransomware attacks. It is therefore evident that the Banks are the most targeted because of their adoption of digital platform in most of their processes, and thus these points to the possibilities of weaknesses in the cyber protection systems. Similarly, the financial cooperatives Sacco's and microfinance institutions are equally affected.

#### **4.5 Chapter Summary**

This section found that the most common reason for individuals and organizations being vulnerable to cyber attack is the ignorance of security measures needed to be taken by the customers and employees of these organizations. Also weak platforms that organizations have set up online are make institutors be vulnerable to breach of information or even monetary loses. This is common in mobile money platforms. Law enforcement has failed to curtail this problem because of inadequate training of not only policemen but judicial officers also have a hard time understanding the technicalities of such issues.

This section found that with the burgeoning use of cyberspace, the internet and digital application, individuals, companies, organizations and even governments have all become increasingly concerned of the dangers of attacks that target the cyber domain or cyber space world. Therefore cyber threats involve the access, use, manipulation, interruption, destruction and physical infrastructure used to process, communicate and store information.

---

<sup>234</sup> Serianu Consultants in Cyber Security (2015); available at <http://www.usiu.ac.ke/oncampus/news/296-serianu-usiu-africa-pkf-consulting-launch-kenya-cybersecurity-report-2015>.

<sup>235</sup> David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017), p. 34.

## CHAPTER FIVE

### SUMMARY, CONCLUSION AND RECOMMENDATION

#### 5.1 Introduction

Chapter five finally sums up the major findings of the research study and hypotheses of the Study. It makes final conclusions and important recommendations on the way forward.

#### 5.2 Summary of the Study

This research aimed to examine cyber terrorism and national security in Africa through the case study of Kenya. The study was prompted by a growing cyber and online threat to Kenya's national security yet there are measures that have been developed to protect the ICT infrastructure. The study sought to why cyber terrorism 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 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.

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 situation awareness 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.

In this modern cyber age, access to information has become too easy. With people putting their personal information on social media plus generally the digital fingerprints people leave online makes finding information about a person relatively easy than it was in the past. Some of this information might be explicitly present online or it can be derived from online resources. That is, information can be gathered from the internet or hackers can use specialized tools to access a person's private network.

### **5.3 Conclusions**

Basing on the objectives of the study and in view of the above findings, the following conclusions are drawn. This research concludes that with the advancement of technology many cyber users have become vulnerable to online attacks and the threats can be overwhelming since they originate from anywhere on the globe. Advancement in technology has also meant that cyber criminals have access to powerful software's that can subvert the security of many networks around the world.

The most worrying thing is that there is a gross lack of awareness of threats posed online by internet users and this is what keeps making hacker careers to keep flourishing. 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. The conclusion here is that with advancement in information technology cyber crime has posed a threat to all facets of modern day life. This manifests itself through things like illegal file sharing of intellectual property, to embezzling of funds online to things like even identity theft.

#### **5.4 Recommendations**

This study thus recommends the following:

Cyber literacy has become almost must for every individual around the world. More and more the world is becoming interconnected by the internet. The internet has become crucial for day to day living whether its accessing government services or ordering of goods or services online and even in crucial things like distant learning. Therefore cyber literacy must make people aware of the dangers that hackers can wreak online and what is at stake if their cyber security is compromised.

It would be cost effective for all stakeholders if cyber security was taught from an early age in schools. Kenya instituted national cyber crime management in order to assess all threats that may lead to crucial cyber information being compromised. And so it is recommended that all stakeholders must come together and cooperate in the fight against this cyber security menace.

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

#### **5.5 Suggested areas of further studies**

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



## REFERENCES

- Akogwu, E. *An Assessment of the Level of Awareness on Cyber Crime among Internet Users in AhmaduBello University, Zaria* (Unpublished B.Sc project). Department of Sociology, Ahmadu Bello University, Zaria, (2012).
- Alexis, O. *SMSs used as a tool of hate in Kenya*, (2016).
- Ayantokun, O. *Fighting Cybercrime in Nigeria: Information-system*.www.tribune.com  
Ehimen, O.R. and Bola, A, (2010), Cybercrime in Nigeria. Business Intelligence Journal, (2010).
- Borg, R. and Gall, D. *Education Research. 6<sup>th</sup> Edition*. New York Longman Inc (1996).
- Brenner, W. *Cybercrime: Criminal Threats from Cyber Space*. Santa Barbara, California: Greenwood Publishing Group, (2010).
- Brinkley, I and Fauth, R. *The Knowledge Economy*, United Kingdom, (2019).
- Burgess, Matt. What is GDPR? WIRED explains what you need to know. Wired, (2018).
- Burt, D., Nicholas, K.S., Scoles, T. *The cyber security risk paradox: impact of social, economic, and technological factors on rates of malware*, Microsoft Security Intelligence Report Special Edition (SIR),Microsoft Corporation, (2014).
- Buzan, B. *Rethinking security after the Cold War*, International Security Studies, (1997).
- Chow, S. *Security Alert Texas through Mexico*, Houston Texas, (2018).
- Christopher, Y. *Intelligence and Security Informatics*, IEEE ISI 2008 international workshops, (2008).
- Chuiyka, A. *Strategies of Cyber Terrorism: Is Cyber terrorism*, Ontario, Canada, (2016).
- Cohen, L and Felson, M. Social change and crime rate trends: A routine activity approach, American Sociological Review, (1997).
- Communications Authority of Kenya, Quarterly Sector Statistics Report: Q2 of the Financial Year 2016/2017.
- Communications Authority of Kenya. First quarter sector statistics report for the financial year 2015/2016.
- Conrad, J. *Seeking help: the important role of ethical hackers*. Network Security, (2012).
- Constitutional implementation in Kenya, 2010-2015: Challenges and prospects, FES Kenya Occasional Paper, No. 5 ISBN: 9966-957-20-0.
- CTED Trends Report (2017), Physical Protection of Critical Infrastructure against Terrorist Attacks, (2017).

- Cyber Defence East Africa 2017 Conference, August 2017 Kampala, Uganda, (2017).
- Daily Nation (2010). Kenya: Alarm as bank employee's siphon out Sh2.4bn through "inside jobs." 10th July 2010.
- Daily Nation. 2015. "Try Crime Suspects Here." Daily Nation, January 15. [www.nation.co.ke/oped/Editorial/ChinaKenya-Hacking-Trial/-/440804/2590722/fcv6r1z/-/index.html](http://www.nation.co.ke/oped/Editorial/ChinaKenya-Hacking-Trial/-/440804/2590722/fcv6r1z/-/index.html).
- David Souter and Monica Kerretts-Makau, "Internet Governance in Kenya: An Assessment for the Internet society, 'Internet society, (2012).
- David, W. *Cybercrime, the Transformation of Crime in the Information Age*, Polity, (2007).
- David, W. *Transformation of Crime in the Information Age*, Washington DC, US, (2017).
- Denning, D. *Cyber terrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Service U.S. House of Representatives*, (2018).
- Dowd, T and McHenry, C. *Security of Networks and the Time to act*, Continental review, (2008).
- Evans. D. *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*. Cisco white paper Cisco Internet Business Solutions Group (IBSG), (2011).
- Fischer, E. *Creating a National Framework for Cyber security: An Analysis of Issues and Options*, February 22, CRS Report for Congress, Order Code, (2005).
- Fischer, E. *History of Critical Infrastructure*, Atlanta Georgia, RL3, (2015).
- Fischer, E. *National Framework for Cyber Security*, SCR Report for Congress, Order Code, (2015).
- 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 world*. (2010).
- Gagliardone, I and Sambuli, N. *Cyber Security 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).
- Heickerd, op. cit., p. 556; Lee Jarvis, Stuart Macdonald and Lella Nouri, "State Cyberterrorism: A Contradiction in Terms?" *Journal of Terrorism Research*, Vol. 6, No. 3 (2015).


- IHS Janes “Adopting a holistic approach to Protecting Critical Infrastructure (2014).
- International Telecommunication Union, “%age of Individuals Using the Internet, 2000 2016,” NB: ITU data published in 2016 retroactively revised its time series data for Kenya’s internet penetration.
- Justine, O. *Growth and other good things*, The Economist, (2013).
- Kagwanja, P. and Karanja, M. How cyber-crime complicates war on terror. The East African, (2014).
- Kamande, W. *The Cyber Crime Society*. Journal of Alternative Perspectives in Research, (2013).
- Kearney, M; Schuck, S; Burden, K and Aubusson, P. *Viewing mobile learning from a pedagogical perspective*. Res arch in Learning Technology, (2012).
- Kenya Cyber Security Report 2016.
- Kenya Vision 2030, (vision2030@kenya.go.ke).
- Kien, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., and Shitanda, S. Kenya CyberSecurity Report 2015. Serianu Limited, (2015).
- Kigen, G. *Kenya cyber security report 2014*, (2014).
- Leverett, E. *Cyber Terrorism Risks and Insurance*. Cambridge Risk Official Center, University of Cambridge, (2017).
- Lewis, J. *Cyber Threats and Cyber Wars*, Washington DC, (2012).
- 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).
- Libichi, B. *Cyber deterrence and Cyber Wars, Laws of Cyber Space*, Atlanta Georgia, RL3, (2018).
- Lorenzo, O. *Challenges of the Modern Century*, Samton Desktops Edition, Atlanta, Georgia, (2019).
- MacAfee 2014, MacAfee Labs Threats Reports. June 2014.
- Maina, Charles. A survey on impact of ICT on Business Value Creation in Kenya Banking Sector. Unpublished MBA project, University of Nairobi, (2010).
- Mallory S, L. *Understanding Organized Crime*, Jones and Bartlett, (2017).
- Mark, M. *Cyber terrorism: Fact or Fancy*, Computer Fraud & Security, Vol. 2 (1998).


- Matinde, V. *High Data Cost and Factors of Mobile Insecurity in Africa*. IDG Connect, (2014).
- Maura Conway, “Reality Check: Assessing the (Un) Likelihood of Cyber terrorism” Springer, (2014).
- Mayssa Zerzri, *the Threat of Cyber Terrorism and Recommendations for Countermeasures*, (2017).
- Michael Erbschloe, *Information Warfare: How to Survive Cyber Attacks* (New York: Osborne/McGraw-Hill, 2011).
- Mutua, W. *The Significance of Mobile Web in Africa and in Future*, (2011).
- Neal K. Katyal, “Criminal law in cyberspace”, *University of Pennsylvania Law Review*, Vol. 149, No. 4 (2001), pp. 1003-1114; Richard W. Downing, “Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime”, *Columbia Journal of Transnational Law*, Vol. 43, No. 3 (2005).
- Newton, B. *Phone Scams of Millions*. Survey of Cyber Crimes in Kenta, Tanzania and Zambia, Herald Cooperation, (2014).
- Nixon Kanali is a trained journalist based in Nairobi. Also founder and editor of Tech Trends KE, (2016).
- Obel, M. *Africa poised for unprecedented, long-term economic growth: Seven drivers that could transform Africa into the world’s economic powerhouse*, *International Business Times*, (2013).
- Patrick Bishop, “Cyber terrorism, Criminal Law and Punishment-based Deterrence” in T. Chen, L. Jarvis and S. Macdonald (eds.), (Abingdon: Routledge, 2015).
- Pawlak, P. *Developing capacities in cyberspace*, in Pawlak, P. (ed.) *riding the digital wave: The impact of cyber capacity building on human development*, (2014).
- Ranz-Stefan Gacy, “Foreign policy: Africa’s internet threat”, *National Public Radio*, (29 March 2010).
- Riis, S. *The Origin of Modern Technology: Reconfiguring Things*. Continental philosophy review, London, United Kingdom, (2019).
- Sarah Gordon and Richard Ford, “Cyber terrorism?”, *Computers and Security*, Vol. 21, No. 7 (2002).
- Schell, B. H. and Clemens, M. *Cybercrime: A Reference Handbook*, ABCCLIO, (2004).
- Schulman, P.R., and Roe, E. *Designing Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures*. *Journal of Contingencies and Crisis Management* Volume 15 Number 1 March 2007.

- Serianu Consultants in Cyber Security (2015).
- Serianu. Kenya Cybersecurity Report 2014. Rethinking cyber security An Integrated Approach: Process, Intelligence and Monitoring, (2014).
- Seymour, B, Kabay, E and Eric, W. *Computer Security Handbook*, 5<sup>th</sup> Ed, John Wiley Inc, New Jersey, (2009).
- Shrekiam, E. *Cyber Crime in North Africa*, the Shape of Future Conflicts, Journal of Crime, (2015).
- Stuart, M. *Cyber terrorism: A Survey of Researchers*, Cyber terrorism Project Research Report No. 1, Swansea University, (2013).
- Susan W. Brenner, “Cybercrime jurisdiction”, *Crime, Law and Social Change*, Vol. 46, No. 4-5 (2006).
- Symantec Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18 (April, 2013).
- Tee Jarvis and Stuart Macdonald, “What is Cyber terrorism? Findings from a Survey of Researchers”, *Terrorism and Political Violence*, Vol. 37, No. 1 (2014).
- The East African. *Kenya launches centre to fight cybercrime*, (2016).
- The Government of Kenya. *CBK Guidance on Cyber Security*, Nairobi, (2017).
- The origins of the term cyber terrorism are typically located in the mid-1980s, see for example: Barry Collin, “The future of cyber terrorism”, *Criminal Justice International*, Vol. 13, No. 2 (1997).
- The United Nation. United Nations *Global Counter Terrorism strategy*. UN, United States, (2016).
- Wanjiku, R. Kenyan banks face challenges with secure online transactions International banks are not as successful as in other markets, (2013).
- Wasuna, Brian. *Taxman, google Kenya in court battle over mystery KRA hack*. The Star Newspaper, Nairobi, Kenya, (2018).
- William A. Wulf and Anita K. Jones, “Reflections on cyber security”, *Science*, Vol. 326, No. 5955 (2009).
- William, M., Mayer, R., and Minges, M. *Africa’s ICT Infrastructure: Building on the Mobile revolution*, World Bank, (2011).
- Wilson, D. *Internet Awareness and Dangers*, Atlanta University, United States of America, (2016).
- Young, J. *The Twenty Four Hour Professor*. The Chronicle of Higher Education, 48, (2016).

## APPENDICES


### Appendices 1: Research License from NACOSTI

  
REPUBLIC OF KENYA

  
NATIONAL COMMISSION FOR  
SCIENCE, TECHNOLOGY & INNOVATION

Ref No: 835082 Date of Issue: 30/April/2020

**RESEARCH LICENSE**




This is to Certify that Mr. ERIC LEE ROTICH of University of Nairobi, has been licensed to conduct research in Nairobi on the topic: CYBER TERRORISM AND NATIONAL SECURITY IN AFRICA: A CASE STUDY OF KENYA for the period ending : 30/April/2021.

License No: NACOSTI/P/20/4860

835082  
Applicant Identification Number

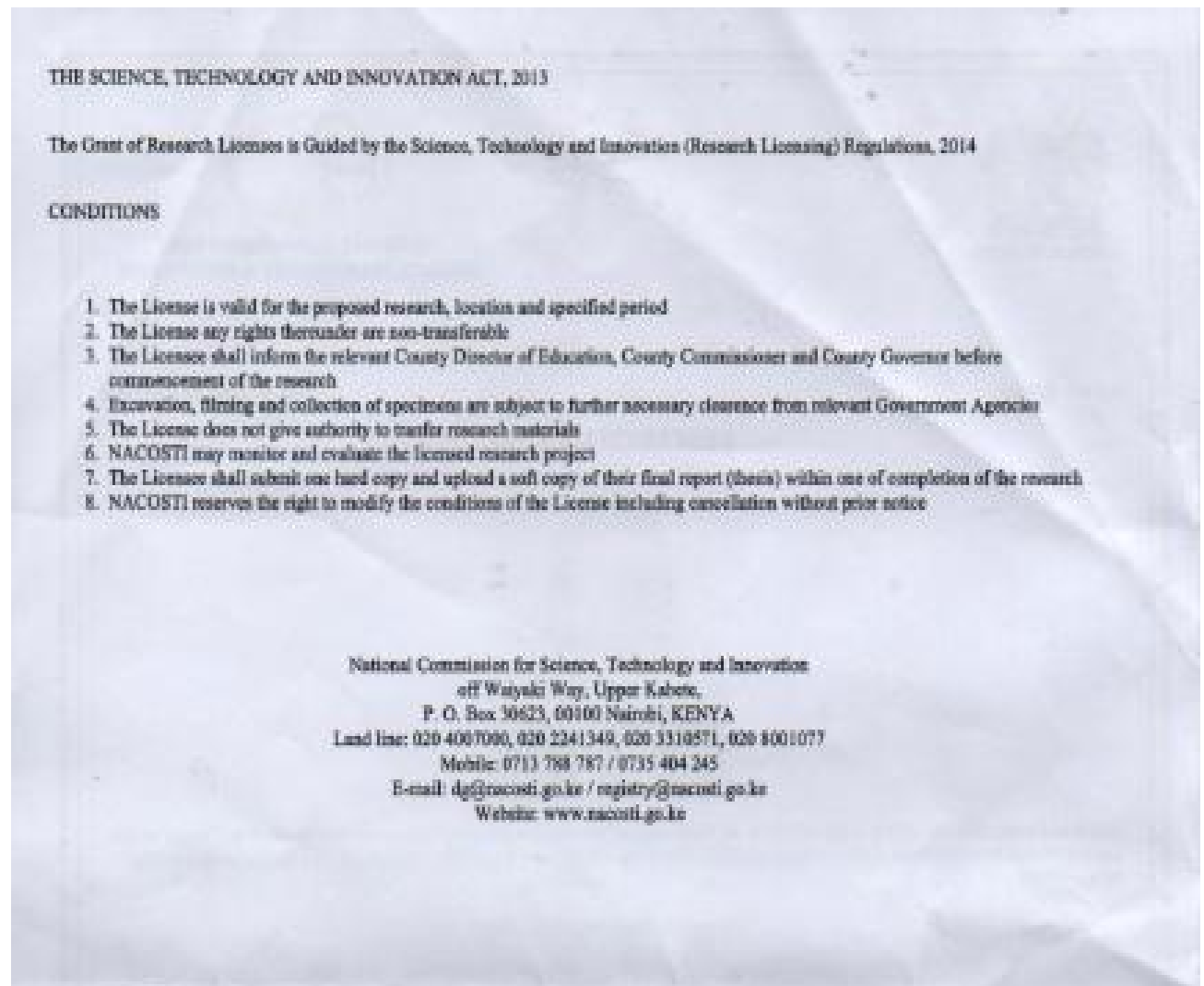
Director General  
NATIONAL COMMISSION FOR  
SCIENCE, TECHNOLOGY &  
INNOVATION

Verification QR Code

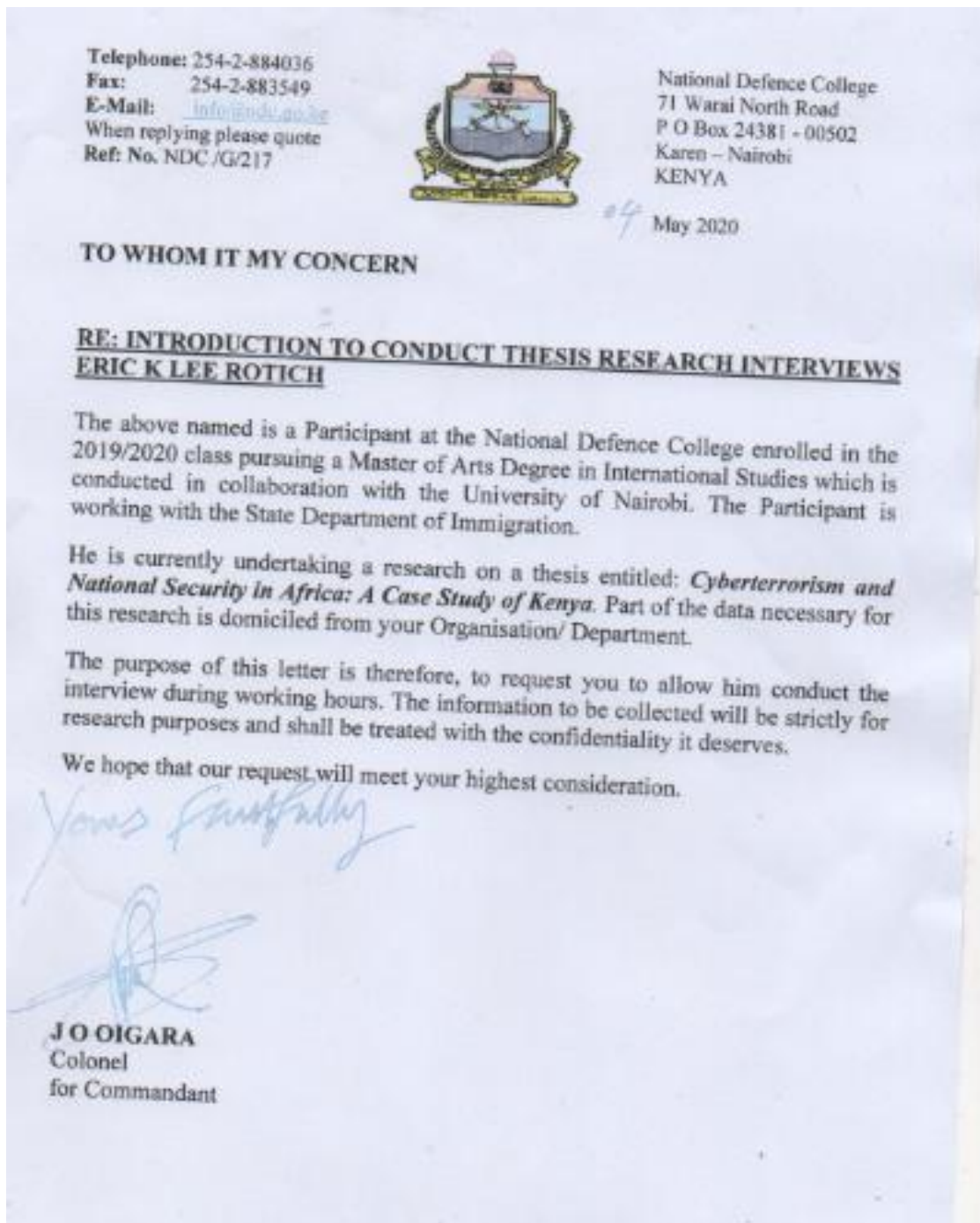


NOTE: This is a computer generated License. To verify the authenticity of this document,  
Scan the QR Code using QR scanner application.

## Appendices 2: Data Collection Permit from NACOSTI



**Appendices 3: Collect Data Collection Authority**





**Appendices 4: Consent Form**

**Consent Form**

My name is ..... I am a student at the University of Nairobi and National Defence College, pursuing a Masters Degree in Diplomacy and International Studies. It is an academic requirement that data is collected as part of research study.

This interview guide is meant to collect information to examine cyber terrorism and national security in Africa using a case study of Kenya, for academic purposes only. Kindly fill this guide to enable me collect data for this study.

Signed Consent.....

## Appendices 5: Questionnaire

Serial: .....

### Research Interview Guide

This research aims to examine cyber terrorism and national security in Africa using a case study of Kenya. The purpose of this interview guide is to collect information from a wide range of informants, who have knowledge about cyber terrorism and national security. It is requested that you please give consent, before you respond.

Clarification on each question can be made where necessarily to your satisfaction. The personal information is optional and kindly note that this work is purely for academic purposes only. Please fill in the questionnaire appropriately. This questionnaire will be submitted to you in hard copy.

#### Instructions

The following statement articulate issues of cyber terrorism and national security. How would you rate some of these statements and give explanations? Where rating scale is 1 = Strongly agree, 2 = Agree, 3 = Un-decided, 4 = Disagree and 5 = Strongly disagree.

#### Section One: Personal Information

Gender? (tick) Male [ ]                      Female [ ]

Age? .....

Occupation? .....

Office / Ministry / Organization? .....

Designation? .....

Duration in employment? .....

Section Two: Cyber terrorism and national security in Africa

Please rate the following statements on cyber technology and insecurity in Africa using the case study of Kenya.

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

1. Do you understand the concept of cyber terrorism? Yes  No

2. Are you familiar with any forms of cyber threats? Yes  No

If yes, which ones?

.....  
.....  
.....

3. Globally, cyber terrorism trends manifest in various ways?

Scale: .....

Explain:

.....  
.....  
.....

4. African continent has faced increased cyber-attacks from extremist elements?

Scale: .....

Explain:

.....  
.....  
.....

5. The forms and nature of cyber terrorism are poorly understood in Kenya?

Scale: .....

Explain:

.....  
.....  
.....

6. Cyber terrorism can result in irreversible damage to critical infrastructure in a state?

Scale: .....

Explain:

.....  
.....  
.....

7. Cyber security experts in your organization have applied varied policy approaches to deliberately tackle cyber terrorism in your organization / institution?

Scale: .....

Explain:

.....  
.....  
.....  
.....

8. Do you think cyber terrorism has serious implications on the Kenya's national security?

Explain:

.....  
.....  
.....

9. Cyber terrorism has many causes in the Kenyan context?

Scale: .....

Explain: (List some of the causes?)

.....  
.....  
.....

10. The multiagency approach is effective in fighting cyber terrorism in Kenya?

Scale: .....

Explain: (Name some of the agencies involved in cyber terrorism)

.....  
.....  
.....

11. What are the possibilities of cyber terrorism attack in your organization?

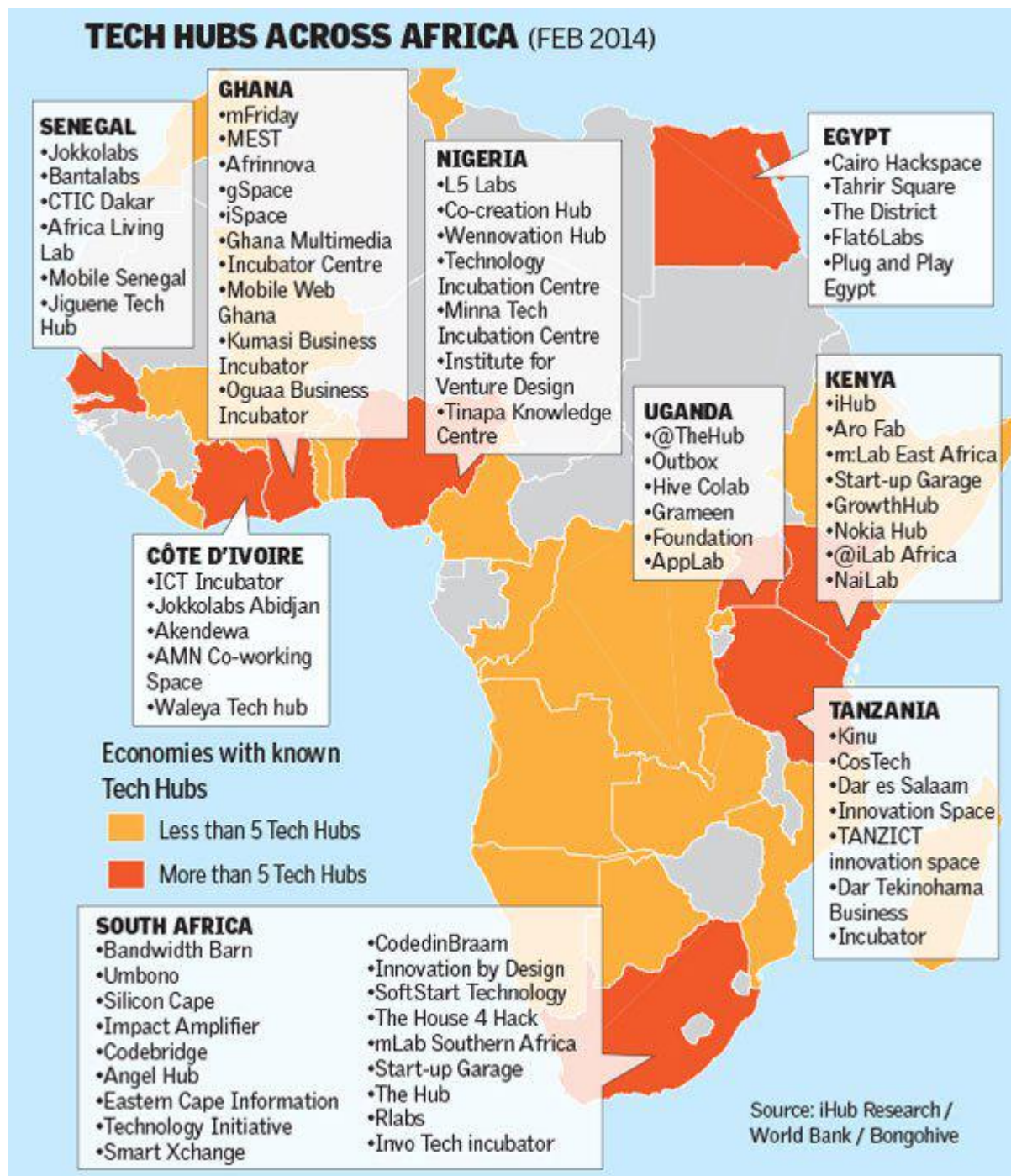
.....  
.....  
.....

12. Why are the chances as stated?

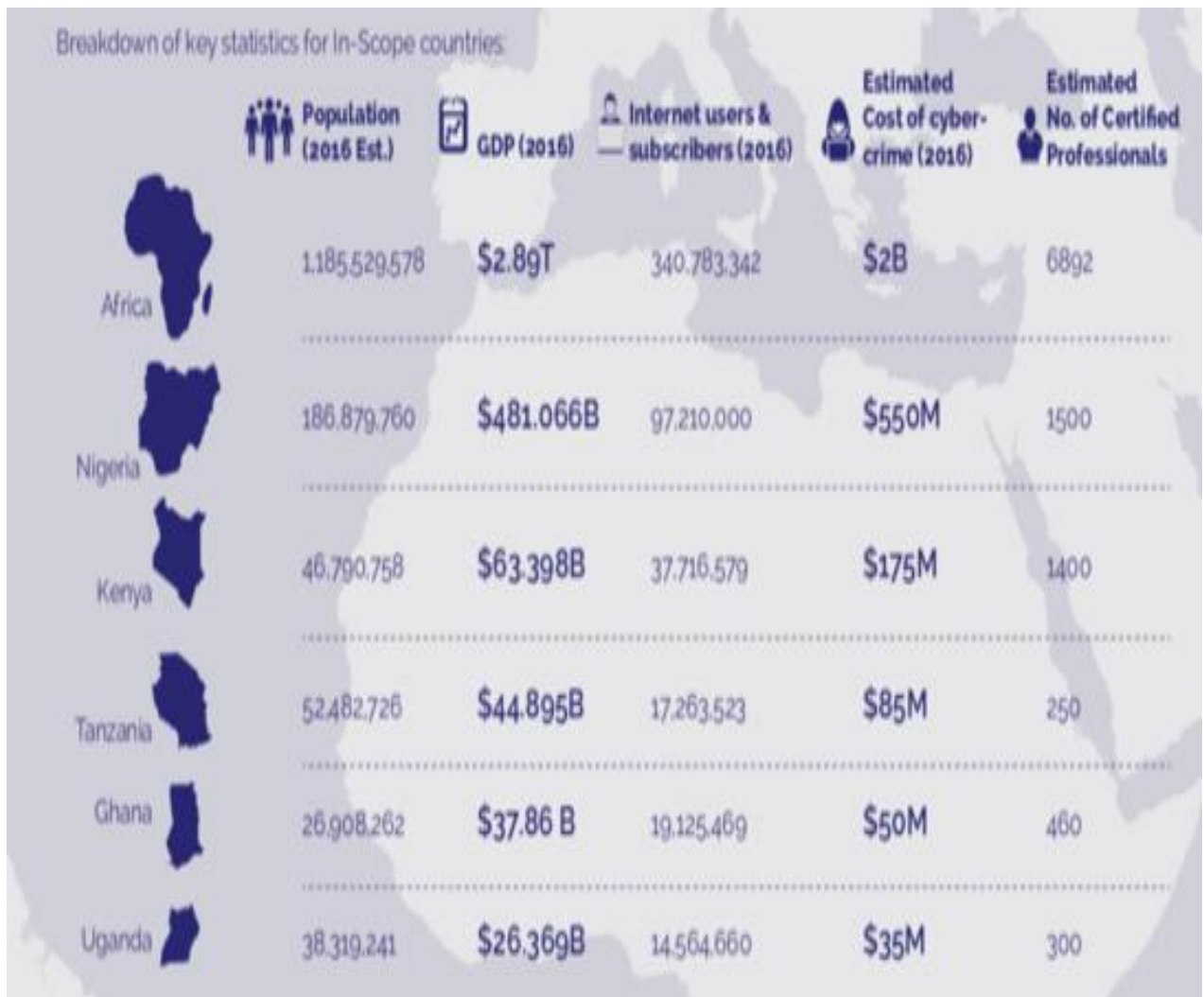
.....  
.....  
.....  
.....



Appendices 6: Study Area Map 1



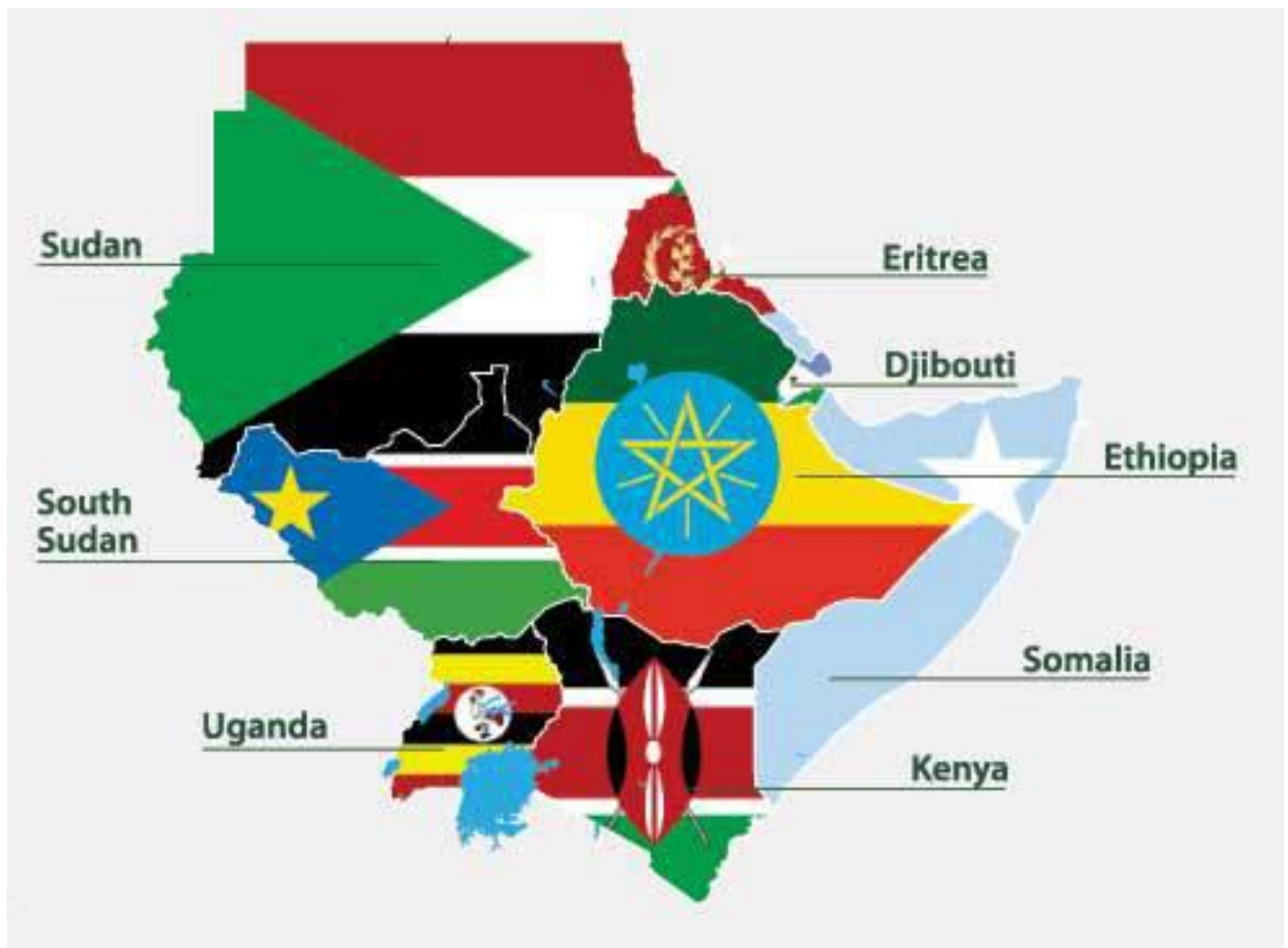
## Appendix 7: Statistics of Information Technology



The map showing cyber threats on African subjects.

Source: Minnaert, Tom. *Footprint or fingerprint: international cultural policy as identity*. *International Journal of Cultural Policy*. Vol. 20 (2014).

**Appendix 8: Study Area Map 2**



This is a map showing the spread of cyber threats in the East African region.

Source: Minnaert, Tom. *Footprint or fingerprint: international cultural policy as identity*. *International Journal of Cultural Policy*. Vol. 20 (2014).



## Appendix 9: Cyber Threats Profiles

Table 16: Cyber threats validated and responded

<i>Cyber Attack Vector</i>	<i>Oct - 17</i>	<i>Nov - 17</i>	<i>Dec - 17</i>	<i>Total</i>
<i>DDOS</i>	1	0	2	3
<i>Domain Impersonation</i>	0	2	2	4
<i>Fake News</i>	3	3	0	6
<i>Malware</i>	10	9	121	140
<i>Online Fraud</i>	8	9	7	24
<i>Online Hate Speech</i>	30	26	6	62
<i>Online Impersonation</i>	26	45	33	104
<i>Phishing</i>	3	2	1	6
<i>Spam</i>	0	1	0	1
<i>System Misconfiguration</i>	14	28	145	187
<i>Website defacement</i>	1	1	0	2
<i>Total</i>	<b>96</b>	<b>126</b>	<b>317</b>	<b>539</b>

*Source: National KE-CIRT/CC*

Cyber threats profile in Kenya.

Source: Kimonye, Mary. *Country Branding: Key lessons and challenges*. Capital FM News, (2013).

## **Appendix 10: Plagiarism Report**

**-END-**