



**UNIVERSITY OF NAIROBI**

**INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES**

**(IDIS)**

**PROMOTING SECURITY IN AFRICA THROUGH EFFECTIVE COUNTER  
CYBER TERRORISM STRATEGIES: A CASE STUDY OF KENYA**

OGONJI MARK

REG. NO. R50/21931/2019

SUPERVISOR:

DR. PATRICK MALUKI

A research project submitted in partial fulfilment of the requirements for the award of Degree of Master of Arts in International Studies at the Institute of Diplomacy and International Studies

**MAY 2019**

## **DECLARATION**

I hereby declare that this research project is entirely my original composition. It has not been presented in any University or College for examination purposes. All references made to works of other persons have been duly acknowledged. Permission from the author and the examining body should be sought before any part of this work is reproduced.

**Ogonji Mark**

**R50/21931/2019**

Signature.....

Date.....

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

**Dr. Patrick Maluki**

Signature.....

Date.....

## **DEDICATION**

This research project is devoted to my family for their invaluable support throughout the study period. I thank Almighty God for giving me the strength and opportunity to carry out the project.

## **ACKNOWLEDGEMENT**

I thank my supervisor, Dr. Patrick MalukI, for his leadership, academic advice and supervision, which has prompted me to complete this project. My family, friends and colleagues thank you for your support and contribution.

## TABLE OF CONTENT

DECLARATION .....	ii
DEDICATION .....	iii
ACKNOWLEDGEMENT .....	iv
TABLE OF CONTENT .....	v
LIST OF FIGURES .....	viii
LIST OF TABLES .....	ix
LIST OF ABBREVIATIONS .....	x
ABSTRACT .....	xii
CHAPTER ONE .....	1
1.1. Introduction.....	1
1.2. Statement of the Problem.....	3
1.3. Objectives of the Study .....	4
1.4. Justification of the Study.....	4
1.5. Literature Review.....	5
1.6. Theoretical Framework .....	8
1.7. Hypotheses of the Study .....	10
1.8. Research Methodology .....	10
1.8.1. Research Design.....	11
1.8.2. Study Site .....	11
1.8.3. Target Population .....	11
1.8.4. Sample size .....	12
1.8.5. Sampling Frame .....	13
1.8.6. Data Collection Methods .....	15
1.8.7. Reliability and Validity .....	15
1.8.8. Data Analysis and Presentation.....	16

1.8.9.	Ethical Consideration .....	16
1.8.10.	Scope and limitations of the Study .....	17
1.9.	Chapter Outline .....	17
CHAPTER TWO .....		19
AN OVERVIEW OF STRATEGIES AND INFRASTRUCTURE FOR COUNTERING CYBER TERRORISM.....		19
2.1	Introduction.....	19
2.2	The evolution of cyber threats .....	20
2.3	Cyber Terrorism Threat .....	23
2.4	The Nature of Cyber Terrorism .....	25
2.5	Strategies to Counter Cyber Terrorism .....	27
2.6	Future Dimension in Counter Cyber Terrorism.....	33
2.7	Chapter Summary .....	35
CHAPTER THREE .....		37
STRATEGIES EMPLOYED TO FIGHT CYBER TERRORISM IN KENYA.....		37
3.1	Introduction.....	37
3.2	Countering Cyber Terrorism and Cyber Extremism.....	37
3.3	Multi Agency Counter Terrorism Strategies and Institutional Capacity.....	43
3.4	Counter Terrorism Financing.....	43
3.5	National, Regional and International Cooperation.....	44
3.6	Cyber Security Measures and Strategies in the Kenyan Perspective .....	45
3.7	Cyber Measures Based on Various Sectors .....	53
3.8	Chapter Summary .....	56
CHAPTER FOUR.....		57
THE CRITICAL ANALYSIS OF EFFECTS OF CYBER TERRORISM ON NATIONAL SECURITY IN KENYA.....		57
4.1	Introduction.....	57
4.2	The Response Rate.....	57

4.3	Demographic Information.....	57
4.4	Nature and Status of Strategies to Counter Cyber Terrorism .....	60
4.5	Cyber Crime and Cyber Attacks in Kenya.....	61
4.6	Causes of Cyber terrorism.....	66
4.7	Strategies to Fight Cyber Terrorism in Kenya .....	68
4.8	Effects of Cyber Terrorism on National Security .....	70
4.9	Chapter Summary .....	73
CHAPTER FIVE .....		75
SUMMARY, CONCLUSION AND RECOMMENDATION .....		75
5.1	Introduction.....	75
5.2	Summary of Findings.....	75
5.3	Conclusion .....	79
5.4	Recommendation .....	83
5.5	Suggestion for Further Studies.....	85
Bibliography .....		86
Appendices.....		94
Appendix I: Letter of Introduction.....		94
Appendix II: Data Collection Instrument.....		95
Appendix III: Questionnaire .....		96
Appendix IV: NACOSTI Research Authorisation.....		105
Appendix V: NACOSTI Permit.....		106

## **LIST OF FIGURES**

FIGURE 1: AGE.....	58
FIGURE 2: LENGTH OF SERVICE .....	59
FIGURE 3: EDUCATION LEVEL .....	60
FIGURE 4: EXPERIENCE OF CYBER TERRORISM .....	67



## **LIST OF TABLES**

TABLE 1: SAMPLE FRAME.....	14
TABLE 2: LIST OF CRIMES .....	63

## LIST OF ABBREVIATIONS

AfDB	-	African Development Bank
AML/CFT	-	Anti-Money Laundering/Countering the Financing of Terrorism
ATM	-	Automatic Teller Machines
AU	-	African Union
AUC	-	African Union Commission
CAK	-	Communications Authority of Kenya
CBK	-	Central Bank of Kenya
CERT	-	Computer Emergency Response Team
CGAP	-	Consultative Group to Assist the Poor
CHRIPS	-	Centre for Human Rights and Policy Studies
CII	-	Critical Information Infrastructure
CIRT	-	Computer Incident Response Team
CT	-	Counter Terrorism
DCI	-	Directorate of Criminal Investigations
DFS	-	Digital Financial Services
DoS	-	Denial of service
EACO	-	East African Communications Organization
ECA	-	Economic Commission for Africa
ECOWAS	-	Economic Community of West African States
ESAAMLG	-	Eastern and Southern Africa Anti-Money Laundering Group
EU	-	European Union
FATF	-	Financial Action Task Force
FIRST	-	Forum of Incident Response and Security Teams
FRC	-	Financial Reporting Center
HRW	-	Human Rights Watch
ICT	-	Information Communication Technology
ICTA	-	Communications Technology Authority
ICTAK	-	Information Communication Technology Association of Kenya
ITU	-	International Telecommunications Union
KDF	-	Kenya Defence Forces
KDN	-	Kenya Data Networks
KE-CIRT/CC	-	Kenya National Computer Incident Response Team Coordination Centre
KECOSCE	-	Kenya Community Support Center
KENET	-	Kenya Education Network,
KEPSA	-	Kenya Private Sector Alliance
KIC	-	Kenya Information and Communication Act
KRA	-	Kenya Revenue Authority
LOAC	-	Law of Armed Conflict
MDA	-	Ministries, Departments and Agencies
MUHURI	-	Muslims for Human Rights

NBK	-	National Bank of Kenya
NCTC	-	National Counter Terrorism Center
NGOs	-	Non-Governmental Organizations
NIS	-	National Intelligence Service
NPS	-	National Police Service
NREN	-	National Research and Education Network
NSCVE	-	National Strategy to Countering Violent Extremism
NTSA	-	National Transport and Safety Authority
NTV	-	Nation TV
ODPP	-	Office of the Director of Public Prosecution
PREACT	-	Partnership for Regional East Africa Counterterrorism
PSP	-	Payment Service Providers
SLAA	-	The Security Laws (Amendment) Act of 2014
SPSS	-	Statistical Package for Social Sciences
STAI	-	State-Trait Anxiety Inventory
SUPKEM	-	The Supreme Council of Kenya Muslims
SWIFT	-	Society for Worldwide Interbank Financial Telecommunication
UNODC	-	United Nations Office on Drugs and Crime

## ABSTRACT

At the heart of cyber-attacks is the threat of terrorism, which is trying to achieve a political effect by creating fear in the population. Kenya, as a society, is becoming increasingly dependent on the Internet in everything from political processes to the economy. This makes cyber-attacks an attractive tool for attackers and also increases the likelihood of cyber-terrorism. There are concerns that the counter-terrorism strategies currently used are traditional and aimed at fighting traditional forms of terrorism, which creates a gap in the absence of appropriate strategies to combat cyber-terrorism. It is this academic gap that is being addressed by this study. The objectives of the study are to examine the nature and state of strategies and infrastructures to combat cyber-terrorism; strategies used to combat cyber-terrorism and the overall effects of cyber-terrorism on national security. This study applies the theory of deterrence, a strategy aimed at forcing the opponent to take a certain course of action or to dissuade him from pursuing unwanted goals. Deterrence is a strategy that uses force and is based on temporary threats designed to influence the opponent, or take a certain course of action, or dissuade him from pursuing unwanted goals. The researcher applied the exploratory approach which involves having an idea or observation which requires further understanding. The data findings identified financial/cyber fraud, hacking, identity theft, phishing and cyber stalking/bullying as some of the cybercrimes prevalent in the country. While Kenya has developed cyber security measures and strategies including legal framework as an important step towards creating a reliable milieu for people and businesses, cybercrime has continued to demonstrate resilience to strike against vulnerable targets. The strategies employed include the multi-agency approach; legislative framework that include the enactment of the Computer Misuse and Cybercrimes Act (2018) which provides the legal mechanism of dealing with cybercrimes including cyber terrorism; capacity building, training and awareness; collaboration with international partners. The study recommends that all stakeholders, including the private sector, play a more effective role in integrating government efforts to address cyber-terrorism threats.; enhance public participation so that law enforcement agencies get a forum to interact with the public whether online or physically as an opportunity to create awareness on the effects of cyber terrorism and build requisite capacity in the law enforcement team to make them responsive to the digital crimes effectively. Further, it recommends the need to implement surveillance and monitoring systems that enable the government to detect those being radicalized through social media platforms. The legislation and training of officials to counter terrorism financing is also key to countering cyber terrorism while the government could have integrated mechanisms to avoid cyber-attacks and alleviate the effects and accelerate recovery if they occur. Establishing a multi-agency counter cyber unit is considered a better way of handling prevention, detection and recovery from cyber terrorism attack.

## CHAPTER ONE

### 1.1. Introduction

Cyberterrorism is a consequence of a nation's level of development and automation of its critical infrastructure. Cyber-terrorism is very attractive to terrorists because of the anonymity involved.<sup>1</sup> Technology has radically changed the security landscape in the world than ever. In that case, cyberspace is not just the Internet, information technology and communications, but a platform that presents unique characteristics, opportunities and challenges as well. Its characteristics are storage, sharing and modification of digital information and data using network or mobile systems. The dimensions of cyberspace are wide since it has coverage that traverses all the way from individuals, communities, cooperation, national to international time and space.

Leverett claims that nowadays everything is in the cyber system and this turns the attention of legal and illegal actions into cyberspace.<sup>2</sup> Some of the cyber activities include cybercrime, cyber defense, cyber war, cyber terrorism, or cyber espionage. Terrorists use cyberspace as their new battleground. Today, terrorism remains a serious problem of concern throughout the world, triggering a heated national debate.<sup>3</sup>

Currently, cyber-terrorism presents a serious and unconventional threat. It is a threat that has no boundaries. It has neither face nor attribution since forces behind it hide behind computers. It is presenting challenges to governments, but there are mechanisms to deal with

---

<sup>1</sup> [http://usiofindia.org/article\\_july\\_sep06\\_9.htm](http://usiofindia.org/article_july_sep06_9.htm)

<sup>2</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>3</sup> Ibid, (2017), p. 17

it. Chow says cyber terrorism is a network attack carried out by a terrorist or an extremist group with the intention of causing physical damage.<sup>4</sup>

Cyber-attacks in Africa are continuously evolving and becoming more dynamic, to a great extent faster than cyber defenses. The advent of information technology has brought with it the emergence of new terror threats previously underestimated such as the threat of cyber terrorism where active terrorist cells all over the world need not travel miles to have a negative impact on the society.<sup>5</sup>

Kenya has a robust Information Communication Technology (ICT) infrastructure which enables it conduct its business in an interconnected world. This research thus seeks to analyze cyber-terrorism threats with a view to recommend effective measures to counter the threat. Terrorism has been sufficiently securitized despite challenges surrounding its definition. Cyber terrorism as an emerging threat requires securitization because it is an existential threat that has no universally accepted definition distinct from cybercrime or cyber-attacks. In addition it has not received adequate attention to harness the synergies required to combat it effectively despite public discourse covering it.

Cyber-terrorism is gaining attention due to the large coverage provided by the media and various institutions.<sup>6</sup> Therefore, it has now become essential to analyze cybernetic terrorism precisely, that is, to study its objectives, motivation and the resources used, in order to develop effective response strategies.

---

<sup>4</sup> <http://www.secure.nsw.gov.au>

<sup>5</sup> Symantec Corporation. *Internet Security Threat Report 2018*, the 2018 Trends, Volume 13 (2018), p. 24.

<sup>6</sup> [https://www.giac.com/practical/GSEC/Shamsuddin\\_Abdul\\_Jalil\\_GSEC.pdf](https://www.giac.com/practical/GSEC/Shamsuddin_Abdul_Jalil_GSEC.pdf)

Based on this scenario, this study predicts that cyber-terrorism will probably represent a more genuine risk to Kenya's prosperity than normal violent terrorism.<sup>7</sup> The cyber war is conceptualized as a state action in a state equivalent to an armed attack. Therefore, this project seeks to bridge the gap in effective and up-to-date strategies against cyber-terrorism.

## **1.2. Statement of the Problem**

Underlying cyber-attacks is terrorism threat that attempts to gain politically by creating fear in the non-military population. While cyber-terrorists have not killed or injured anyone or damaged critical infrastructures, it is not possible to determine whether this is due to operational deficiencies or to the protection systems and capabilities used by Kenya. The Kenyan society has become increasingly dependent on the internet as automation continues in various sectors of the economy. The level of automation makes cyber-attacks attractive for malicious actors to inflict harm and also increases the chances for the possible occurrence of cyber terrorism.

The Government of Kenya considers national cyberspace security among the top national priorities in ensuring that her citizens are secure from attacks. The critical infrastructure which refers to the physical and virtual assets or facilities, private or publicly owned are essential to the provision of vital services to Kenya, for their social and economic wellbeing.

There is concern that the counter terror strategies currently being applied are traditional, and are geared towards combating traditional forms of terrorism, thereby presenting the gap on lack of appropriate strategies against cyber terrorism. It is this academic gap that this study addressed. To do this, the study was based on three research questions, that is, what is the nature and status of strategies and infrastructure for countering cyber terrorism?; What

---

<sup>7</sup>Ivita Kīsnica, Organization and individual security: Collective Monograph, [https://www.theseus.fi/bitstream/handle/10024/153249/Organisation\\_and\\_Individual\\_Security.pdf?isAllowed=y&sequence=1](https://www.theseus.fi/bitstream/handle/10024/153249/Organisation_and_Individual_Security.pdf?isAllowed=y&sequence=1); <https://ruor.uottawa.ca/>

strategies have been implemented to fight cyber terrorism in Kenya?; and What are the common consequences of cyber terrorism for national security?

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

The aim is to explore how security can be achieved in Africa through effective cyberterrorism strategies in Kenya. The specific objectives include:

- 1.4.1 To examine the nature and status of strategies and infrastructure for countering cyber terrorism.
- 1.4.2 To determine the strategies employed to fight cyber terrorism in Kenya.
- 1.4.3 To analyse general effects of cyber terrorism on national security in Kenya.

### **1.4. Justification of the Study**

Cyber-terrorism is a relatively maturing branch of knowledge in its advancement and has been related with the state as well as individuals.<sup>8</sup> The study is expected to spawn new knowledge that will help in promoting security in Africa through effective counter cyber terrorism strategies particularly in Kenya.

#### **1.4.1. Policy Justification**

This study aims to enlighten the policy makers on the need to sharpen their skills further on structural and operational performance for better functioning of national cyber security systems. While Kenya has suffered conventional terrorism for some time, and has adopted measures to confront it, the possibility of a shift from conventional terrorism to cyber-terrorism presents a security gap.

---

<sup>8</sup> Demessie Fantaye, "Horn of Africa Bulletin, November-December 2015" Volume 27 Issue 6



### **1.4.2. Academic Justification**

The intention is to contribute to academic works on emerging trends and patterns of cyber terrorism, which could be useful to scholars and academicians dealing with the subject matters, especially given the ever expanding dynamism of cyber-attacks today.<sup>9</sup>

## **1.5. Literature Review**

In this section, a number of scholars have made attempts to differentiate the subjects of cyber space, cyber threats, and national security. In addition, the sub-sections further reviewed the current theoretical literature and empirical literature relating to cyber terrorism incidences, the types of threats, effects on national security<sup>10</sup> and possible solutions to the emerging cyber terrorism challenges.

### **1.5.1. Cyber terrorism**

There have been various attempts made at defining cyber-terrorism with no convergence yet. The difficulty in arriving at a definition stems from the fact that it is a phenomenon that is not easy to identify and apportion intention. Chuipka (2016) argues that the convergence between the digital world and the physical world results in a sort of vulnerability.<sup>11</sup> This helps determine the definition of computer terrorism.<sup>12</sup> Cyber terrorism can be an attack with a political intent based on technology.<sup>13</sup> It can damage infrastructures such as government registers, medical records, financial and commercial infrastructures in a highly automated environment developed by Kenya and risks related to IoT devices.

---

<sup>9</sup> <https://www.ijmsh.com/articles/eBOOK%20for%202015FINALII.pdf>

<sup>10</sup> [https://www.giac.com/practical/GSEC/Shamsuddin\\_Abdul\\_Jalil\\_GSEC.pdf](https://www.giac.com/practical/GSEC/Shamsuddin_Abdul_Jalil_GSEC.pdf)

<sup>11</sup> Chuipka, Adam. *The Strategies of Cyberterrorism*. (Ottawa, 2016), p. 1.

<sup>12</sup> Ibid; <http://www.usrlib.info/>

<sup>13</sup> Chuipka, Adam. *The Strategies of Cyber Terrorism*, Ottawa, Ontario, (2016), pp. 89-91.

Dorothy Denning says “Cyberterrorism is illegal and access or attacks against computers systems, networks as well as information stored in them with the intention of coercing individuals or governments to support their goals.”<sup>14</sup> The cyber-attacks are directed at computer systems and the information which are critical government assets. Cyber-terrorism may result in physical harm against persons or property. It is therefore a threat to the security of a country.<sup>15</sup>

### **1.5.2. Nexus between Cyber Terrorism and National Security**

The use and application of technology, access to information and the use of social networking has provided an enabling platform for manipulation and dangerous desires.<sup>16</sup> There is an increase in politically motivated cyber-attacks that target nation-states. Therefore, if a cyber-attack causes loss of lives or property it may be considered an armed attack that requires military response.<sup>17</sup> The military would definitely use force as a means of last resort to defend the country against cyber threats by operating in a non-military capacity.<sup>18</sup> Theoretical underpinnings guiding discussion of cyberterrorism are social network theory, game theory and deterrence theory.

### **1.5.3. Social Network Theory and Game Theory**

Social network theory involves terrorists operating in all types of networks with interconnections for sharing and dissemination of information. Internet chat rooms operate in an interconnected environment. Similarly, computer and information security experts as well

---

<sup>14</sup>Denning D. E., *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. <http://www.nautilus.org/info-policy/workshop/papers/denning.html>

<sup>15</sup> <https://ccdcoe.org/>

<sup>16</sup> NATO Cooperative Cyber Defence Centre of Excellence. *2018*

<sup>17</sup> Ibid

<sup>18</sup> Ibid

as law enforcement professionals need to engage in in the same all-network communication channel to counter cyberterrorism.

In terms of game theory, individuals are placed in circumstances that they have to interact with others. It's about a player getting to know the decision made by their opponents in order to decide which decision to take. For example, in cyberterrorism, cyber attackers undertake illegal activities believing it will lead to alternative courses of action that prevent them from reaching their ultimate goals. They thrive on self-glorification. That is, any action that causes damage to computer systems and networks, gives them a sense of triumph. The counter strategies employed by computer professionals maybe retaliatory or conciliatory in nature.

#### **1.5.4. Deterrence Theory**

The theory of deterrence<sup>19</sup> is a strategy based on temporary threats aimed at influencing the enemy so that he can take certain actions or dissuade them from pursuing unwanted goals.<sup>20</sup> Deterrence can be viewed as convincing your opponent that the costs and / or risks of a particular procedure that can be taken is higher than its benefits.

It involves both elements of control and power with ultimate impact on the international sphere. It has been associated with military power or use of force<sup>21</sup>. It has been adequately used in preventing a nuclear war.

Theorists have therefore placed deterrence at the centre of counter cyberterrorism as well as prevention and defence against cyber-attacks.<sup>22</sup> In the traditional deterrence approach, it succeeded in stopping mutually assured destruction. The theoretical underpinnings of

---

<sup>19</sup> Álvarez, José Manuel Saiz. "Group Cyberpreneurs and Virtual Social Networks in the Post-Industrial Technology Cybersociety (CTP)." pp. 533–535

<sup>21</sup> Schelling (1980).

<sup>22</sup> Austin Long, *Deterrence: From Cold War to Long War* (Santa Monica: RAND, 2008), 5, [http://www.rand.org/pubs/monographs/2008/RAND\\_MG636.pdf](http://www.rand.org/pubs/monographs/2008/RAND_MG636.pdf).

deterrence is based on game theory in which there is a belief that unilateral military build-up breeds a sense of fear that would cause the potential adversaries to restrain their hostile actions. This assumes that potential belligerent is normal and is capable of performing a cost benefit analysis so as to make the right choice. Among the theories identified, deterrence theory is found useful to counter cyberterrorism.

## **1.6. Theoretical Framework**

Theory of deterrence was used to explain the need for nuclear weapon and that owning nuclear arsenals prevented countries from going to war. This can also be applied to cyberspace, as cyber deterrence. It became a tool of engagement during the Cold War period. It is a Latin word, "dēterrere", which means "to frighten or turn away". Deterrence is about preventing adversaries from causing harm to their opponents. It is about having defensive mechanisms and restraint for fear of the consequences.

Deterrence differs from compellence in that deterrence seeks to prevent someone not to do something, while compellence seeks to encourage someone to take a certain course of action. Deterrence depends on intention and ability to achieve desired result. However, it suffers from the inconsistency in the ability to discern the intention and threats.

Deterrence involves both elements of control and power with ultimate impact on the international sphere.<sup>23</sup> The debate on the prevention of expansion became known at the end of World War II when use of force became a means to defeat the enemy. It became a major component of means of negotiating power used to avoid wars through coercion and threats. The change in the understanding of use of force made it amenable to deterring nuclear war.

---

<sup>23</sup> Gaycken, Sandro, and Maurizio Martellini. Cyber as Deterrent. In Deterrence and IT Protection for Critical Infrastructures, edited by Maurizio Martinelli, 1-10. Heidelberg: Springer, 2013

The theory of punitive deterrence was advanced by the first classical philosophers such as Cesare Beccaria<sup>24</sup> and Jeremy Bentham.<sup>25</sup> They disagreed with the legal position of European thinking as well as the spiritualistic explanations of crime. They then postulated and gave modern deterrence theory grounding in criminology.

The theoretical underpinnings of deterrence is based on game theory in which there is a belief that unilateral military build-up breeds a sense of fear that would cause the potential adversaries to restrain their hostile actions. This assumes that potential belligerent is normal and would choose the best option.

Conceptually, deterrence has been applied to modern security issues that involve terrorism with some degree of success.<sup>26</sup> Furthermore, deterrence is cheaper than constant conflict. Cyber attacks could cost lives in situations where states include cyber warfare in normal operations<sup>27</sup> Although IT apologies require new capacities, these costs are lower than the temporary loss of the network or financial markets.<sup>28</sup> The conflict leads to human and material costs that can be avoided if deterrence is applied.<sup>29</sup>

Jeremy Bentham argues that individuals are rational and can undertake a cost benefit analysis before acting. There are substantial reservations about this rational actor model, since other models such as bureaucratic politics and group think may override choice of best alternative options.

---

<sup>24</sup> Beccaria, C. (1963).

<sup>25</sup> Bentham, J. (1948).

<sup>26</sup> Paul K. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counter-terrorism: A Component in the War on al-Qaeda* (Santa Monica: RAND, 2002), [http://www.rand.org/pubs/monograph\\_reports/MR1619/MR1619.pdf](http://www.rand.org/pubs/monograph_reports/MR1619/MR1619.pdf).

<sup>27</sup> Shane Harris, The Cyberwar Plan: It's Not Just a Defense Game; Cyber-Security Includes Attack Plans Too, and the U.S. Has Already Used Some of Them Successfully, (*National Journal*, 14 November 2009), [http://www.nationaljournal.com/njmagazine/cs\\_20091114\\_3145.php](http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php).

<sup>28</sup> Peeter Lorents, Rain Ottis, and Raul Rikk, Cyber Society and Cooperative Cyber Defence, a paper presented at the 3rd International Conference on Internationalization, Design, and Global Development, (San Diego, CA 2009), p. 184.

<sup>29</sup> Long, *Deterrence*, 17–22, 59–61, explains this phenomenon at length, as does Libicki, *Cyberdeterrence and Cyberwarfare*, pp. 32–35.

Freedman provides a wider explanation by incorporating narrow and broad deterrence; central and extended conceptions which cover parties not part of the conflict but who may be affected by the actions of the offender. He also distinguishes between actions that require immediate or general deterrence especially during crisis situations.<sup>30</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. Analysts fear the rise in cyber-attacks in Kenya could be a prelude to a larger assault that could impact local businesses and the broader economy.

### **1.7. Hypotheses of the Study**

**H1:** The failure to adopt effective cyber terrorism strategies has led to increased insecurity in Africa

**H2:** The adoption of relevant cyber terrorism strategies will reduce incidences of attacks in Kenya

**H3:** The cyber-terrorism strategies employed in Kenya apply a multi-agency approach.

### **1.8. Research Methodology**

Research methodology is an operational framework where data is analysed in order to clearly interpret the meaning intended.<sup>31</sup> Research methodology is multi-dimensional in which it explains the logic for applying certain research methods or techniques.

---

<sup>30</sup> Ibid

<sup>31</sup> Leedy, Paul. *Practical Research*. New Jersey: Prentice-Hall, (1997), p. 1.

### **1.8.1. Research Design**

Exploratory approach is being used in this project where the researcher has an idea or observation that requires further understanding. The research approach provides the basis for future research or determination of the availability of theory for current observations.

The research style is being carried out where there is little or no prior research on the research problem. The aim is to gain an understanding of basic details, conditions and problems, the development of preliminary theories or assumptions, the definition of usefulness of the study.

In addition, this study uses a mixed approach, that is, qualitative and quantitative approaches. Mixed research is helpful because it has improved research results. The combination of qualitative and quantitative approaches reinforced the rating. This has allowed the balance between limiting different data and the benefits of others.

### **1.8.2. Study Site**

The acts of cyber terrorism transcend global, regional, national and local boundaries. Therefore this study is conducted in Kenya, but with a specific focus in Nairobi County which possesses the most automated critical infrastructure that is susceptible to cyber terror.

### **1.8.3. Target Population**

The target population includes key experts in terrorism, ICT and national security. The respondents will be key stakeholders in cyber security who will include, Kenya Defence Forces, National Police Services, National Counter Terrorism Center, Immigration Department, Information and Communications Technology Authority (ICTA), Kenya Prison Service, Kenya Civil Aviation, Ministry of Foreign Affairs, National Intelligence Service.

#### 1.8.4. Sample size

The sample size is set by identifying the number of observations necessary for the statistical sample. It is a key feature of empirical research, whose purpose is to draw conclusions about the totality of the sample.<sup>32</sup>

According to Kothari, the total sample size can be achieved by calculating using the Fisher formula.<sup>33</sup> Selecting a sample and coming up with the sample size can be simple or complex based on the sample size.<sup>34</sup> The formula listed below is used to calculate the appropriate sample size in the prevalence study.

$$n = \frac{Z^2 p(1 - p)}{d^2}$$

Here n is the size of the sample, Z is the statistic corresponding to the confidence level, P is the expected value and d is the precision.<sup>35</sup> The confidence level, which is usually calculated, is 95 percent. Most researchers present the results with a 95% confidence interval (CI).<sup>36</sup>

Calculating the sample size is useful when planning a study. This is representative of the number of respondents participating in the study. The sample size will be estimated at the 95% confidence interval (z = 1.96), the population share is set at 20% (p = 0.2) and the desired accuracy level is 10% (d = 0.1) as follows;

$$n = \frac{(1.96)^2 \times (0.2) \times (0.8)}{(0.1)^2} = 61.47 \text{ (approx)} = 61$$

---

<sup>32</sup> Anthony G. Turner (2003).

<sup>33</sup> Kothari, C. R. 2004. *Research methodology: methods & techniques*. New Delhi: New Age International (P) Ltd. <http://public.eblib.com/choice/publicfullrecord.aspx?p=431524>.

<sup>34</sup> Ibid, (2004), p.11.

<sup>35</sup> Ibid, (2004), p. 15.

<sup>36</sup> "Mugenda, Abel and Mugenda, Olive. *Research methods dictionary*. Nairobi, Kenya arts press, (2012), pp. 12-13."



The target population was found to be less than 10,000, which necessitated the adjustment of the sample size using the following formula:

$$nf = \frac{n}{1+n/N}$$

Where:

nf = the desired sample size

n = the calculate sample size

N= the total population (estimated at 80).

Therefore,

$$nf = \frac{61}{1+61/80} = 34.61 \text{ (approx)} = 35 \text{ respondents}$$

### **1.8.5. Sampling Frame**

The sample structure refers to the various elements that make up the population of interest and may include individuals, families or institutions. Therefore, for this survey, a total sample size of 35 is considered adequate. The selected sample is 61 percent and the target sample is used. Targeted sampling is a type of non-probabilistic sampling, which is more effective when it comes to studying a specific cultural field with experts in the field of terrorism and security. Objective sampling can also be used with quantitative and qualitative research methods.

Selecting a targeted sample is of fundamental importance to the quality of the data collected, so ITU's reliability and competence are guaranteed. This can be achieved by dividing the target audience into appropriate units, age, competence, background, functional areas, departments and subsequent random sample used to select the actual participants in the research based on the proportional size of the subgroup. This method is applied to ensure

that all the elements of the population are duly represented in the research. This assisted in removing bias on the samples chosen which would have negative affects to the outcome of the study. Such biases would likely negatively affect the quality of data and the resultant study findings of this research. Therefore where  $n=35$  is applicable to a population not exceeding ten thousands (10,000). Hence for a population of 61 respondents then the formula applies to generate the sample size in Table 1.

<b>Category</b>	<b>Target Population</b>	<b>Percentage (%)</b>	<b>Sample Size</b>
National Counter Terrorism Centre	6	10	2
Kenya Defence Forces (Counter-Terrorism Unit)	6	10	2
National Police Service ( Anti-Terrorism Police Unit)	10	16	7
ICT Authority	4	7	2
Ministry of Foreign Affairs	5	8	3
National Intelligence Services	10	16	7
Ministry of Interior	7	12	3
University Students(Youth)	8	13	3
Private Sector	5	8	1
<b>Total</b>	<b>61</b>	<b>100</b>	<b>30</b>

*Table 1: Sample Frame*

*Source: Author, (2018)*

### **1.8.6. Data Collection Methods**

The data were obtained from primary and secondary sources. Primary data was collected through interview guides.<sup>37</sup> As noted by Kothari, qualitative data is best collected by researchers through interviews. As a result, this study employed key informant interview as a more powerful tool in eliciting narrative data that allows researchers to investigate respondents' views in greater depth.

The key informant interview guide through a structured questionnaire was aimed at key stakeholders in cyber security who included Kenya Defence Forces, National Police Service, National Counter Terrorism Center, Immigration Department, Kenya Prison Service, Kenya Civil Aviation, Ministry of Foreign Affairs, National Intelligence Service, County Commissioner Office and State Law Office. The purpose of interviews with key informants was to obtain information from a wide audience, which has a direct understanding of effective strategies against cyber-terrorism.

In addition, secondary data was collected from information security related sources, such as books, magazines, articles and periodicals. This has greatly helped to capture accurate information that has allowed us to generate new knowledge or simply verify and confirm from previous analyses of cyber terrorism. Secondary data is selected based on the date of publication, the author's credentials and the reliability of the source.

### **1.8.7. Reliability and Validity**

Reliability and validity is assured through improvement of the analysis instrument by reinforcing its internal consistency by pre-testing the research tool. The necessary measures have been taken to ensure the research is carried out in accordance with institutional

---

<sup>37</sup> <http://docplayer.net/33090211-Errors-in-sample-surveys.html>

guidelines according to institutional guidelines. In addition, content validity was established through consultations and discussions with the research supervisor as a specialist in the area of research topic. Finally the consistency of data was achieved by examining raw data and reducing data to meaningful attributes.

### **1.8.8. Data Analysis and Presentation**

It should be noted that data collected was interpreted using document and thematic analysis techniques. Document Analysis is a qualitative study that includes the interpretation of a document that gives meaning to its content.

Thematic analysis<sup>38</sup> is a qualitative research method used to examine and record the models within the data. Organize and describe the data set in more depth. The subject acquires vital attributes associated with information related to the search query and represents a certain level of response or value in the data set. The coding system was used to simplify the information. The statistical package for social sciences (SPSS version 23),<sup>39</sup> was used for data analysis. Descriptive statistics<sup>40</sup> in the form of averages, standard deviations and percentages were also used to analyze the quantitative data.<sup>41</sup> The results are presented in the form of frequency tables, histograms and diagrams.

### **1.8.9. Ethical Consideration**

The research adhered to procedures established with all sources being acknowledged. Before administering questionnaire, the interviewer requested and obtained consent. Respondents made a choice whether to participate in the survey or not. Maximum confidentiality was

---

<sup>38</sup>Mark Widdowson, British Association for Counselling and Psychotherapy.

<sup>39</sup>*SPSS Tutorials*, [www.spss-tutorials.com/spss-what-is-it/](http://www.spss-tutorials.com/spss-what-is-it/).

<sup>40</sup>Ibid

<sup>41</sup>Ibid

maintained, especially in the management of the questionnaires to ensure anonymity. This also required seeking permission from NACOSTI.

#### **1.8.10. Scope and limitations of the Study**

The study was carried out between June 2018 and June 2019 within Nairobi County. One of the limitations of the study was finding experts in the field because of the sensitive and technical nature of the area under study. This was mitigated by focusing on the key departments dealing with the research area.

Self-reported data from the target population was also a challenge, thus the researcher took time to properly orient the prospective respondents during the interviews, and in addition this study provided all the necessary research support document, non-disclosure agreement and clear consent forms during data collection process. The researcher therefore was cognizant of potential bias from respondents and took measures.

### **1.9. Chapter Outline**

#### **Chapter 1: Introduction**

The first chapter is the introduction. It establishes a theoretical framework of the topics covered and, in particular, of what has been studied, why and how.

#### **Chapter 2: The Nature and Status of Strategies and Infrastructure for Countering Cyber Terrorism**

Chapter two illustrates the 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 3: The Strategies Employed to Fight Cyber Terrorism in Kenya**

Chapter three gives an elaborate background of strategies employed to fight cyber terrorism in Kenya. This chapter also describes the theoretical concepts underpinning cyber terrorism and its relationship with insecurity.

### **Chapter 4: Critical analysis of the impact of cyberterrorism on national security in Kenya.**

It presents an analysis of Cyberterrorism's influence on national security in Kenya and further addresses the issue of cyberterrorism security in Kenya.

### **Chapter 5: Summary, conclusion and recommendation**

Finally, chapter five summarizes the main results as per the objectives of the study. It makes several key conclusions and important recommendations on the way forward.

## CHAPTER TWO

### AN OVERVIEW OF STRATEGIES AND INFRASTRUCTURE FOR COUNTERING CYBER TERRORISM

#### 2.1 Introduction

This chapter discusses the various strategies and infrastructures needed to combat cyber terrorism. Cyber terrorism can be neutralized by using different mechanisms before or after it occurs. In theory, terrorists could benefit from society's growing dependence on information technology that gives them access and even the ability to paralyze critical sectors such as military or financial services. This emerging threat has social, political, economic and religious roots that require strategies that effectively address the threat. Cyberterrorism fuses two spheres, terrorism and technology which are critical concepts that require more proactive rather than reactive approaches.

The end of the cold war<sup>42</sup> brought globalization and the impact of information technology in national and international security sectors. Examples include the high level of IT skills deployed by US troops in the first Gulf War (1990-1991) and the global nature of media coverage, especially in the conflicts in Somalia (1993) and the Balkans (1992-99). There have also been cases of system failures as a result of hacker activity, as evidenced by the cyber-attacks that struck Estonia in May 2007 and the increasing use of Internet for cyber warfare by al-Qaida and other actors. The dependence of developed states on information technology puts their systems at risk of being used as cyber weapons and attack targets.

---

<sup>42</sup> J. Boone Bartholomees--National Security Policy and Strategy

To help in understanding and determining effective strategies and the thinking behind them, theoretical considerations are addressed. This involves an analysis of deterrence theory and its consequent effect on cyber terrorism.

Various reasons have been given for cyber-attacks with financial being the key one.<sup>43</sup> Evidence also shows cyber-attacks have become more political. Meanwhile, cyber-terrorists know that governments are dependent on the network and, therefore, have found ways to exploit it.<sup>44</sup>

## **2.2 The evolution of cyber threats**

Technology has connected devices, people, organizations, institutions and governments like never before. Therefore, it is important to appreciate from the beginning that cybernetic technology generally refers to many devices from desktop computers, computer networks, communications and Internet technology or cyberspace.

Lee emphasizes that a very connected world offers new opportunities and challenges. In general terms, the cyberspace is a combination of databases, networks and information sources into a data warehouse. Cyberspace, therefore, is not a virtual system per se, but also includes computers, servers, satellites and cables. Siang-tse and Jayakumar have discovered that most researchers tend to use the terms cyberspace and the Internet almost interchangeably even if the Internet is just one of the elements in cyberspace.<sup>45</sup> Cybercrime, also known as cybercrime, is a vice that mainly involves computers and takes place within cyberspace.

---

<sup>43</sup> <https://en.wikipedia.org/wiki/Cyberterrorism>

<sup>44</sup> Ibid

<sup>45</sup> Siang-tse, Foo and Jayakumar, Shashi. *Cyber Threats: 2018 and Beyond*, Rajaratnam School of International Studies, NTU. (2018), pp. 2-3.



Siang-tse and Jayakumar also point out that in 2018 there was a surge in cyber-attacks worldwide, particularly targeting critical infrastructures.<sup>46</sup> Transport, energy and medical institutions are the objects of choice, since the interruption of the service could provoke a severe reaction from the public. States should take note that the adoption of computer technology, however good it may seem, involves many security risks, since hackers will have an infinite attack surface to attack.<sup>47</sup>

Boey argues that cyber threats are becoming a growing international concern. For instance, WannaCry ransomware attack in May 2017 demonstrated the potential for global cyber-infection events, as reported in more than a hundred countries.<sup>48</sup> The NotPetya malware had also incidences in over a hundred states as well, clearly illustrating the far-reaching consequences of the evolution of cyber threats deep into the global system.

According to Burgess<sup>49</sup>, repeated attacks on global financial systems such as the World Interbank Telecommunications Society (SWIFT) have hit several states with the capacity to undermine the financial system worldwide. Furthermore, the proliferation of crypto-coins and anonymization techniques fuel the spread of cyber threats. According to Thomson, states are using their cyber capabilities to achieve geopolitical goals. An attack on Ukraine was sponsored by the state. The attacks spread and go beyond the borders.

Cyberspace has emerged as a focal point of geopolitical tensions. The cyber actors of North Korea declared to have exfiltrated the joint operational plan of the United States and South Korea 5015 containing plans on how to invade North Korea. Another example is represented

---

<sup>46</sup> Ibid. (2018), pp. 2-7.

<sup>47</sup> Chappell, Bill. *'Petya' Ransomware Hits at Least 65 Countries; Microsoft Trace it to Tax Software*. NPR. (2018), pp. 5-8.

<sup>48</sup> Boey, Darren. *North Korean Hacker Group Linked to Taiwan Bank Cyber Heist*. Bloomberg Technology. (2017), pp. 8-12.

<sup>49</sup> Burgess, Matt. *What is GDPR? WIRED explains what you need to know*. Wired, (2018), pp. 12-19.

by the growing tensions within the biggest nuclear confrontation since the missile crisis in Cuba.

The cyber technology has had huge impact on how Africa conducts its business. Africa has witnessed an increased internet penetration in the last decade. However, as the continent digitalize its business processes, the potential attack by cybercriminals become more complex.<sup>50</sup> The attackers target weaknesses in the technology infrastructure and processes leading to huge loss of finances and valuable information systems. This threat has made Africa rethink how it can better leverage the benefits derived from cyber technology use by building capacity. However, this projection will be difficult to achieve unless serious discussions on the need to solve the challenges presented by the spread of the Information Communication Technology (ICT) infrastructure and Internet applications will be considered.

According to ITU report of 2014, the growth of ICT in Africa has been progressing upwards compared to countries of Asia and Latin America. Cyberspace is an intrinsic part of the growth of any state and yet, on the African continent it is the most subject to attacks. 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.

The new Africa, as contained in the expression “Africa Rising” is mirrored in the continent’s increasing acceptance of mobile technology.<sup>51</sup> The continent is characterized by rapid development in information communication technologies (ICT) in the public and private sectors. This was possible thanks to independence in the sector in which both companies and

---

<sup>50</sup> Kenya Cyber Security Report, (2016), p. 14.

<sup>51</sup> John, O.S., (2013), p. 108.

individuals compete freely in the market. The rapid developments in technology while positive require cyber secure systems that are more resilient to attacks.

### **2.3 Cyber Terrorism Threat**

In the academic community, discussions and different opinions about cyberterrorism and its impact on national security are in progress. This disagreement is linked to different concepts of cyberterrorism. The concept of cyberterrorism as a form of terrorist activity on the Internet gives it more chance to appear than a more opaque and restrictive definition.<sup>52</sup> Consequently, cyber terrorism may be viewed as unauthorised access and infiltration of computer, networks and data they contain through the use of threats, intimidation or coercion against a government or its citizens for political or social purposes. For any attack to qualify as cyberterrorism, it should not solely cause damage that generates fear within the public, but also violence against persons or property. Vital national infrastructure may be a target of attack that might be the act of cyberterrorism.

Cyberterrorism could be a relatively recent addition to the security domain, as academic literature is emerging around this development. The study of this development is dominated by three important questions. These concerns definition, importance and types of response to the current threat.

There are four options regarding the disagreements scholars realize with the term cyberterrorism. First feature is that the form of conduct needed for an act to be considered cyberterrorism. In a very broad sense, it encompasses terrorists' on-line activities that include radicalization, communication and attack designing, fundraising, coaching and propaganda. The second feature called into question is the damage shown. Collin describe cyber-terrorism

---

<sup>52</sup> Lee Jarvis, Stuart Macdonald, *Locating Cyberterrorism*, 2014.

as "hack a body count", that is, the attack must generate physical violence against people; there are arguments against accepting significant economic or environmental effects or even online. The third concern has to do with the intention or reason for the attack. Holt argues that cyber-terrorism should not be completely linked to fear, but also attempts to show terrorists use the Internet since it is suitable for cyber-crimes. The fourth and final point concerns the agents involved in the act. There are those who believe cyber-terrorism is the work of non-state actors while states are involved in cyber warfare and cyber espionage. However, researchers believe that states are also able to participate in cyber-terrorism.

Thus, cyberterrorism may overlap with traditional terrorism, cybercrime, or cyber war. However, when the attack is economically motivated than ideologically, it is considered cybercrime. A scholar like Erbschloe<sup>53</sup> in the study of information warfare explores the connection between economy and national defense. Conway in his research reflects whether the terrorist groups operating in cyberspace are "cyber-terrorists". He believes that this depends on the concept and on what constitutes cyber-terrorism, considering that defining terrorism is rather problematic. The distinction between cyberterrorism and cybercrime would be crucial in determining where the perpetrators of cyberattacks fall.

Academics are not in tandem when it comes to the extent of the threat of cyber terrorism in relation to the damage that cyber terrorists can inflict. Others argue that the existence of network vulnerabilities can increase their personal online interactions. Wilson, for example, is concerned about zero-day exploits, that is, codes that fully exploit unknown vulnerabilities in computer systems. Skeptics argue that cyber-terrorism remains unlikely as a top most type of cyber-attacks, in relation to traditional physical attacks; outsourcing attacks. Others argue

---

<sup>53</sup> Michael Erbschloe, *Review of Information Warfare*, [www.techsoc.com/warfare.htm](http://www.techsoc.com/warfare.htm).

that, according to the cost-benefit analysis, the value of cyber-attacks perpetrated related to physical attacks remains high.

Researchers have focused on the responses to cyberterrorism which continue to elicit considerable debate. Development and enactment of legal mechanisms to combat cyberterrorism is an area under discussion; however their effectiveness within the domestic environment is questionable. Cyberterrorism legislation faces the problems of attribution and jurisdictional scope and the cyber-attacks are such that they transcend several jurisdictions which call for international cooperation.

## **2.4 The Nature of Cyber Terrorism**

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, a cyberspace war, or cyberterrorism.<sup>54</sup> As a rule, cyber warfare involves states and can be equated with armed attack or use of cyber-force, which may require a military assault.

There is ongoing debate as to the real threat of cyberterrorism with various opinions saying its exaggerated and that its destructive and harmful effects may not merit concern. However, both media and government operatives are of the view that terrorists have acquired the capability to use Internet for various cyber operations such as radicalization, fundraising, recruitment and carry out cyber-attacks.<sup>55</sup> However, no record or data exist showing that terrorist organizations have mounted success attacks against systems and networks, however reports indicate that many terrorist organizations have acquired capability and capacity to

---

<sup>54</sup> Matt Burgess, *What is GDPR?*, 2018, pp. 12-19.

<sup>55</sup> Mayssa Zerzri, *Cyber Terrorism Threats and Countermeasures*, (2017)

carry out cyber-attacks.<sup>56</sup> This kind of threat requires that policy makers and security planners design and implement preemptive actions to prevent such attacks from occurring.

According to routine activity theory, cyber threats thrive when there is availability of suitable opportunities and the lack of adequate protection measures. Translating this theory to cyber technology, shows that the ICT evolution is not without challenges. The advancing nature and falling costs of ICT has given rise to digitalization of economies in Africa. The internet has fundamentally transformed the continents political, economic and social lives. The growing technological exposure offers its own vulnerabilities and risks. Africa's flourishing economies have an undisputable link to the achievement of technology on the continent. Nevertheless, these advances give way to the threat of hacking, cybercrimes and malware. Cyber security is now a growing concern to the continent. As technology evolves, so is the nature and prevalence of cyber threats. With businesses trying to find better ways to link with their customers, cyber security presents a huge risk with potential to compromise client loyalty and trust. These risks are seen in the way in which cybercrime is defying every prescription.

Susan W. Brenner contends that cyber threats were first heard in 1990s in Ghana, Africa. This is the period that internet and private computers began to be sophisticated and universal.<sup>57</sup> She claims that cybercrime has come from the advances in technology and cybercrime, which is perceived as a crime that occurs in networks.<sup>58</sup> Cybercrime is one of the major threats to national security in the world and is one of the main priorities of INTERPOL at the international level.

---

<sup>56</sup> Ibid

<sup>57</sup> Susan W Brenner, *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: Praeger, 2010.p 38.

<sup>58</sup> James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Cyber Threats*, (2002), pp. 22-27.

According to Symantec Corporation report (2013)<sup>59</sup>, the cybernetic threat is a growing global phenomenon that is developing faster in Africa than in the rest of the world. Cyber Security experts claim that 80% of computers in Africa have viruses and other malware.<sup>60</sup> Statistics from various sources paint Africa as an environment is susceptible to attacks because of its the vulnerable networks and systems. According to the Norton Cyber-Crime Report 2016<sup>61</sup>, for every second there are 20 people suffering from cybercrime, which means more than 1.5 million deaths per day in Africa.<sup>62</sup>

The Symantec report of 2016 indicates that cyber-attacks in Africa grew by 42 percent.<sup>63</sup> Understandably, 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. Similarly, major cities in the continent which are well served with IT have experienced cyber-attacks especially in industries, security and financial sectors.

## **2.5 Strategies to Counter Cyber Terrorism**

Criminals, terrorists and spies depend to a large extent on cyber technologies to support the organization's objectives and, consequently, the rapid identification and mitigation of threats, including the permanent monitoring of networks, applications and devices, through an internal security operations center or an external service is needed.<sup>64</sup> There are possibilities that states may sponsor cyber-terrorism for political and national interests. While there is high level of anonymity, a cyber-attack could still be traced to its source.

---

<sup>59</sup> Symantec Corporation, (2013).

<sup>60</sup> Ranz-Stefan, G. Foreign policy: Africa's internet threat, National Public Radio, (2010), p. 29.

<sup>61</sup> Norton Cyber-Crime Report, (2016), p. 79.

<sup>62</sup> Symantec Corporation, (2016), p. 107.

<sup>63</sup> Ibid, (2012), p. 126.

<sup>64</sup> Siang-tse, Foo and Jayakumar, Shashi. *Cyber Threats: 2018 and Beyond*, Rajaratnam School of International Studies, NTU. (2018), pp. 2-3.

Arrests and prosecution of cyber criminals is still quite low. There is however a new drive to apply the legal instruments in prosecuting cybercrimes.

In 2018, several high-profile malicious program writers were sent to prison. They include Marcus Hutchins, "the hero of WannaCry". He was sentenced to 40 years in prison for his role in creating and distributing the Trojan Kronos from 2014 to 2015. A number of countries have enacted legal instruments necessary for handling cybercrime.

### **2.5.1 Cyber Legislation**

Most African countries have domesticated the African Union (AU) counter-terrorism strategy. It promotes linkages and understanding in the fight against terrorism. The AU Summit held in Equatorial Guinea in June 2014 adopted the Convention on the Security of Cyberspace and the Protection of Personal Data and the governments authorized to access individual data without the permission of the owner. This is because national security is the preserve of the government and hence member states should create protection mechanisms to fight cybercriminals.<sup>65</sup>

On the basis of these facts, most African states have adopted different strategies to contain the threats peculiar to their environment. Most African nations 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 adherence to the AU Convention.

---

<sup>65</sup>Judith M. C. Tembo, "Workshop on Tanzania National Transposition of SADC Model Law", 4th–5th February, 2013.



## 2.5.2 Cyber Deterrence

It must be understood that in the fight against cyber terrorism it is difficult to understand even the consequences of cyber-weapons. A malicious code attack would obviously spread across the web attacking not only the intended target, but all vulnerable systems. This could have a serious effect on essential infrastructure systems as well as those of partner states. There are many arguments as to whether deterrence can be effective against cyber-terrorism.<sup>66</sup> Jim Lewis claims that deterrence is not possible in the cyber region. He argues that the asymmetric nature of the attack, the resulting enemies, and the difficulty in responding to the source of an attack prevent effective deterrence.

Deterrence refers to the process of influencing an adversary to avoid a certain course of action in its own interest.<sup>67</sup> The theory of cyber deterrence involves the application of military force or other actions against any possible opponent to discourage them from any cyber terrorism attacks. Deterrence in the cyber domain is complex, but according to Colin Gray, "deterrence can work, but when it does, it's the adversary's vision of the world which determines whether deterrence is successful or not".<sup>68</sup>

According to the theory of deterrence, deterrence is more applicable when the threat of using force is real. This usually happens during the war and is governed by the Armed Conflict Act (DCA), also known as the War Code. LOAC is a part of international law governing the

---

<sup>66</sup> Oliphant, Roland and McGoogan, Cara. *NATO warns cyber attacks 'could trigger article 5' as world reels from Ukraine hack*. The Telegraph. (2017), pp. 91-21.

<sup>67</sup> Schelling, Thomas, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), p. 9.

<sup>68</sup> Collin Gray, *National Security Dilemmas*, 2011, p. 56.

conduct of armed conflicts (*jus in bello*).<sup>69</sup> The LOAC is therefore relevant to the response to terrorism as well as cyber terrorism.

The LOAC ensures that damages and harm to victims of any conflict are minimized; protect both fighters and non-combatants; protect rights of combatants and non-combatants; and facilitate the restoration of peace after the end of the conflict. LOAC is based on principles of military obligation and legal pursuit. The military obligation considers the use of force proportional to the threat that leads to the partial or total submission of the enemy at minimum cost to the army.<sup>70</sup>

The second principle is the legal orientation which is based on three assumptions: there is a limit to the right of a belligerent to hurt the enemy; civilian populations will not be targeted; and a clear distinction between fighters and non-combatants to avoid endangering non-combatants.<sup>71</sup> This principle requires that there is deliberate action to ensure only military objects are targeted while civilian population is protected.<sup>72</sup>

In Article 51 of the Charter of the United Nations, collective self-defense is recognized as the inalienable right of one or more States.<sup>73</sup> It is used as a means of preventing conflicts or protecting the allies when intimidation fails.

---

<sup>69</sup> U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication pp. 1–02 (Washington, DC: November 8, 2010), 214, available at: [http://ra.defense.gov/Portals/56/Documents/rtm/jp1\\_02.pdf](http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf).

<sup>70</sup> Geoffrey S. Corn, Victor Hansen, Richard Jackson, Christopher Jenks, Eric Talbot Jensen and James A. Schoettler, *The law of armed conflict: An operational approach*. Volume 94 Number 886, 2012

<sup>71</sup> *Ibid*

<sup>72</sup> *Ibid*

<sup>73</sup> Article 51, *Charter of the United Nations and Statute of the International Court of Justice* (San Francisco, CA: United Nations, 1945), available at: <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>.

### 2.5.3 Cyber Dissuasion

Dissuasion is a strategy discourages and influences leadership of potential adversaries from initiating military competition.<sup>74</sup> Dissuasion occurs before a threat manifests itself. It involves using non-military approach especially during peacetime.<sup>75</sup> Dissuasion is used to convey the message of futility of an action.<sup>76</sup> With dissuasion, then one would avoid deterrence action.<sup>77</sup>

Resilience involving use of redundant network hardware and Internet connectivity pathways is key recovery during a potentially devastating cyberattack. The establishment of resilience with proper mitigation measures makes an adversary to determine that cyber-attack would not produce desired results. This may cause the adversary to discard such action and search for alternatives.

Dissuasion requires building a cyber defence and cyber forensics capability. The cyber forensics, the science of gathering evidence from computer systems to determine the source and target of cyber-attack is a critical tool for law enforcement agencies in their investigations. Forensics capabilities apply “electronic fingerprints” or other tools to determine what happened following a cyber-attack.<sup>78</sup>

Finally, dissuading cyber-terrorism involves process of interdicting and stopping the funding of terrorism activities.<sup>79</sup> It is recognized that funding is essential to support the activities

---

<sup>74</sup> Department of Defense, *Annual Report to the President and the Congress* (Washington, D.C.: 2002), 18.

<sup>75</sup> Chairman, Joint Chiefs of Staff, *Combating Weapons of Mass Destruction*, JP pp. 3–40 (Washington, D.C.: Department of Defense, June 10, 2009).

<sup>76</sup> *Ibid* pp.1-3

<sup>77</sup> Gray, *National Security Dilemmas*, 2011, p. 59.

<sup>78</sup> Chen, *Cyberterrorism after Stutxnet*, p. 4.

<sup>79</sup> U.S. Department of State “Counter Threat Finance and Sanctions,” *State.gov*, available at: <http://www.state.gov/e/eb/tfs/>.

terrorist organisations. The government's efforts must be directed towards financial transactions whether coming from states or non-state actors.<sup>80</sup>

#### **2.5.4 Cyber defence**

Cyber Defense is a defense mechanism used to protect critical infrastructure.<sup>81</sup> Its main task is to prevent and detect cyber-attacks. This ensures the security of confidential information as well as property. Cyber security is ensured by threats and increases system and network security.

#### **2.5.5 Concession**

This is a way of relaxing tensions by giving in to some demands so as to avoid war.<sup>82</sup> While employing this counterstrategy, it must be based on the interests of the nation. Cyberterrorism is not easy to apply. This is because it may spread to targets that were not the subject of attack.

#### **2.5.6 Retaliation**

The government may employ retaliation when its interests are under threat.<sup>83</sup> But retaliation in cyberspace may not have the intended results. Thus, states may use other measures other than the cyber tools.

#### **2.5.7 Passive Defence**

A state put controls in place to minimize costs the terrorist organization can inflict. This involves eliminating any vulnerability in the systems and networks terrorists may exploit. If

---

<sup>80</sup> Ibid

<sup>81</sup> NATO Cyber Cooperative Cyber Defence Center of Excellence Tallin Estonia. <https://ccdcoe.org/cyber-definitions.html>.

<sup>82</sup> Kydd and Walter, "The Strategies of Terrorism,"p.64

<sup>83</sup> Ibid

there are no vulnerabilities, then cyber terrorism would not succeed. While it is not possible to fully secure all likely targets,<sup>84</sup> this strategy is one of the best to pursue.

### **2.5.8 Deny Terrorists Access to Cyber Weapons**

It is important for states, especially those that have nuclear and biological weapons to ensure they do not fall into the hands of terrorists.<sup>85</sup> The strategy can also be applied to cyber weapons that are sold in the dark web. There are challenges states face when it comes to cyber domain. Some of the tools like zero day exploits used in the Stuxnet virus are readily available, including the means of producing them.<sup>86</sup>

### **2.5.9 Psychological**

Terrorism has a psychological effect on society, but states have the responsibility to ensure its implications are maintained at the minimum.<sup>87</sup> When people are exposed to cyber terrorism, they experience anxiety, stress related issues and insecurity. Therefore, governments could employ the same strategy to have a psychological impact on terrorists by denying them publicity.

## **2.6 Future Dimension in Counter Cyber Terrorism**

Cyber criminals do acquire huge sums of money from their illegal activities. However, they face huge challenges when trying to monetize the funds. This is because monetization of such

---

<sup>84</sup> Matusitz p. 168.”

<sup>85</sup> Kydd and Walter, “The Strategies of Terrorism,” p. 65.

<sup>86</sup> Wilson, Cyber Threats to Critical Information Infrastructure, p.131.

<sup>87</sup> Kydd and Walter, The Strategies of Terrorism, p.65.

proceeds would involve money laundering.<sup>88</sup> They also face hardened financial systems whose measures are designed to keep cyber-attacks away.

Oliphant and McGugan say sustainability efforts, such as those that cover excess network equipment and Internet connectivity, promise significant improvements after a widespread and potentially destructive cyber-attack. With improvements in cyber resilience and a determination to make cyberspace secure may influence an adversary not to undertake a cyber-attack as its effects may not produce the desired results.<sup>89</sup>

According to Heavey, the internet penetration in Africa is rising at a faster rate than the average in the world. Criminals in the industry have therefore taken advantage and are cashing in on the opportunities by stealing online bank account details.<sup>90</sup> Automatic Teller Machines (ATM) frauds and hacking have been prevalent in the banking sector and other sectors of the economy. More importantly, African business and customers are deeply engaged in online business activities, which provide criminals with opportunities to strike. According to information telecommunications and mass media, there were more than 300 million data subscribers in Africa in 2015. The research conducted by ICT Advice in Kenya in 2010 showed that 18 percent of Kenya's students buy music / movies and 24 percent buy e-books online.<sup>91</sup>

In the past, the African economies relied on sidelight links which was slow, but with the coming of fibre optic cables, there is booming business.<sup>92</sup> Due to the old link, the connectivity was unreliable and business unattractive. However, the situation has drastically

---

<sup>88</sup> “Chappell, Bill. *‘Petya’ Ransomware Hits at Least 65 Countries; Microsoft Trace it to Tax Software*. NPR. (2018), pp. 5-8.”

<sup>89</sup> “Oliphant, Roland and McGoogan, Cara. *NATO warns cyber attacks ‘could trigger article 5’ as world reels from Ukraine hack*. The Telegraph. (2017), pp. 91-21.”

<sup>91</sup> Juma V. (2010). [Http://www.businessdailyafrica.com](http://www.businessdailyafrica.com).

<sup>92</sup> Kinyanjui, K. (2009b). *Increasing Cybercrime Threat*. [Http://www. Businessdailyafrica.com](http://www.Businessdailyafrica.com)

changed with the coming of the 3G fibre optic connectivity across Africa and the entire world. This digitalization process has presented new security challenges to the continent.<sup>93</sup> For example, in 2009, Kenya experienced over 800 boot attacks per day. However, according to Safaricom daily record log sheet (unpublished), over 17 million attempts are encountered each day. This clearly point at a growing broadband access, globalization of viruses and malware products.

This phenomenon explains the state of Africa's crime rate associated with digital activities mainly in the social media as a clear pointer to an existing gap in the continent's digitalization programme. Case in point is the use of face book which is the highest visited website by over 15 percent users and is known to be the most popular crime zone presently. Other sites that have motivated cybercriminals are associated with selfish motives. Crimes that have been reported based on such motives include cyber bullying in South Africa,<sup>94</sup> cyber-attacks on the website of Uganda, Kenya Police and Kenya Airways. Similarly, individuals reportedly used hate speech in form of short text messages is frequently seen in Kenya.

## **2.7 Chapter Summary**

This chapter argues that the dark web and the proliferation of cyber weapons is a catalyst for cyber-attacks. These tools make it easy for cyber terrorists to target vulnerable systems and networks. It also shows that strategies exist to mitigate any possible cyber-attack. The response to an attack does not need to be military, but may encompass nonmilitary actions, such as economic or financial measures.

---

<sup>93</sup> Ibid, (2010), p. 23

<sup>94</sup> Gesser, U., Maclay, C., and Palfrey, J. (2010). Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations, an Exploratory Study by Barkman Center for Internet and Society at Harvard University in collaboration with UNICEF.

Ultimately, a strategy applied to prevent cyber terrorism must make it clear to the adversary that it would not be in their best interest to engage in the intended course of action as the cost would not be worth it. This preventive strategy must be pursued as the most critical means of avoiding war, however, when it fails, then use of force may be considered. This strategy represents a all-inclusive tactic to address the threat of cyber terrorism. The following chapter analyzes strategies used to combat cyber-terrorism in Kenya.



## CHAPTER THREE

### STRATEGIES EMPLOYED TO FIGHT CYBER TERRORISM IN KENYA

#### 3.1 Introduction

In the previous chapter, the nature and state of strategy and infrastructure for combating cyber terrorism, particularly in Africa, were discussed. The chapter was defended by strategies that prevent cyber-terrorist attacks. To address the second goal of this study, this chapter discusses strategies developed to counter cyberterrorism in Kenya. It further deals with strategies used to deal with terrorists in cyberspace based on cyber defence distinguished as either passive or active defense.

#### 3.2 Countering Cyber Terrorism and Cyber Extremism

To counter cyber terrorism and cyber extremism, different actors have been examined to determine the measures used in the fight against vices.

##### 3.2.1 The Social Media and Internet

The social media has become an attractive tool for terrorists in their effort to recruit and radicalise its sympathisers. Terrorist groups such as ISIS and al-Qaida are currently using cyber-crime, where they share videos and hate the Internet with the aim of radicalizing and creating a new generation of cyber-jihadists.<sup>95</sup> Thus, it becomes a virtual platform for strengthening extremist attitudes and acting as an echo.

McKenna and Bargh<sup>96</sup> (1998) argue that cyberspace and terrorism are linked, allowing terrorists to use the internet for terrorist purposes. With this statement, critics argue that this

---

<sup>95</sup> Imran Awan, (2017) Cyber-Extremism, <https://doi.org/10.1007/s12115-017-0114-0>

<sup>96</sup> McKenna, & Bargh, 1998.

means that web sites and sites of social networks have become a safe haven for potential extremists to "care" for vulnerable people.

Social networks, such as Facebook and Twitter, have a positive and negative impact on society. People do business, communicate and stay in touch through such platforms. The sites are also attractive to terrorists as places for recruitment and radicalisation. However, they can also be used by governments to propagate its narrative as a counter cyber-terrorism strategy. The role of the media needs to be enhanced to help in counter-terrorism operations. The Kenya government in partnership with the media fraternity and other stakeholders has focused on efforts to reduce access to media tools and is conducting surveillance of social networking sites to prevent abuse by cyber criminals.

### **3.2.2 NGOs and Civil Society**

Mary Kaldor (2003) argues that NGOs and civil society are critical as they shape opinion and public views in the society.<sup>97</sup> The groups have been vocal as defenders of human rights and humanitarian law to which both governments and the terrorists are required to observe. By engaging with local communities, civil society can influence the youth and other vulnerable groups from joining extremist organisations. They can also counteract the narratives of radicalization and counter the unilateralist war approach pursued by states.<sup>98</sup>

The civil rights groups are at the forefront in defending rights of accused persons including that of terrorists.<sup>99</sup> However, accusations abound that civil society groups are quick to defend the rights of suspected terrorists, but fail to respond when civilians as well as security personnel are killed during terror attacks.

---

<sup>97</sup> Kaldor, M. (2003). *Global Civil Society: Answer to War*. Polity Press, Cambridge. pp. 149-158

<sup>98</sup> Ibid

<sup>99</sup> Choi, S. W. (2010). Fighting terrorism through the rule of law? *Journal of Conflict Resolution*, 54 (6), pp. 940-966.

NGOs and the Kenyan government have been working closely to reach the various communities where terrorist activities are high. NGOs can be used to promote anti-radicalisation measures targeting the youth who are most vulnerable. The association between the government and the NGOs in de-radicalization creates safe "contact points" for relatives, friends and neighbours who concerned about those already radicalised.

The NGOs have supported social programs that provide safety nets for those without gainful employment to prevent them from being lured into crime and possibly terrorist activities. Kenyan civil society organisations have been able to monitor and document any possible violations of suspect's rights thus ensuring CT operations are within the legal limits.

### **Kenya Community Support Centre (KECOSCE)**

KECOSCE, founded in 2006 has participated activities that has made the communities resilience against terrorism. It helped to identify radicalized young people, including those facing radicalization or recruitment. It has also provided psychological and community support. It continues to monitor and report on online content that may be used to radicalise and recruit people into violent extremism.<sup>100</sup> KECOSCE participates in television and radio programs on awareness of radicalization and public awareness of peace.<sup>101</sup>

Furthermore, KECOSCE supports unemployed and underemployed youth through education, training and internships. It promotes governance which guarantees the provision of basic services, including the mounting of anti-corruption campaigns.

---

<sup>100</sup> Marshall Center., PTSS 16-12 Participants Study Civil Society's Role in Defeating Terrorism, Counter Terror Financing. (2016).

<sup>101</sup> "Kenya Community Support Centre., Kecosce Annual Report - 2013 - (KECOSCE, 2013). Retrieved 23 December 2018, from [http://www.kecosce.org/downloads/kecosce\\_organizational\\_annual\\_report\\_2013.pdf](http://www.kecosce.org/downloads/kecosce_organizational_annual_report_2013.pdf)"

## **The Supreme Council of Kenya Muslims (SUPKEM)**

SUPKEM founded in 1973 has provided both social and economic support to the Muslim population through the partnerships with government agencies, donors and communities. SUPKEM is actively involved in counter terrorism efforts. It is part of the National Charter for Promotion and Responsibility to Combat Violent Extremism.<sup>102</sup> It provides training to religious leaders impressing upon them the narrative on religious tolerance and not extremism. As a religious body it has been in the forefront championing religious harmony and co-existence. As a strategy, there is need to have a link is to harness the efforts of NGOs in reaching vulnerable youths who may be enticed into using cyber weapons to mount attacks.

### **3.2.3 International Partners**

#### **The Regional CT Law Enforcement project**

The Regional CT Law Enforcement project is a four-year regional project funded by the European Union (EU). Its goal is to strengthen collaboration on CT issues and organize regular policy exchanges. The key values of respect for the rule of law and international human rights inform the project and the project supports them as an essential basis for police investigations, legal actions and judicial proceedings.

#### **Partnership for Regional East Africa Counter Terrorism (PREACT)**

Partnership for Regional East Africa Counter terrorism (PREACT) is a multi-year program that supports the United States. It seeks to create strong institutions in the civilian and security sector, to build strong capacities and to eliminate the circumstances that contribute to

---

<sup>102</sup> “International Center for Counterterrorism., National Workshop on Countering Incitement and Violent Extremism in Kenya | ICCT. (2014). Icct.nl. Accessed 23 December 2018, from <https://icct.nl/update/icct-works-with-un-cted-on-counterterrorism-in-nairobi/>”

the spread of violent extremism, the efforts needed to enable governments of host countries to assume the responsibility for combating terrorism.<sup>103</sup> These areas include the reduction of combat capabilities of terrorist networks; the development of the rule of law in combating terrorism in partner countries; increased border security; stopping the financing of terrorism and reducing the attractiveness of radicalization and participation in violent extremism.

PREACT partner countries are Djibouti, Ethiopia, Kenya, Somalia, Tanzania and Uganda, Burundi, Comoros, Rwanda, Seychelles, South Sudan and Sudan.

### **3.2.4 Kenya – USA Partnership**

The Kenyan authorities were interested in the scope of capacity-building programs supported by the US government, subsidized and updated by the departments of State, Defense, National Security and Justice. The projects included the preparation of an emergency response, border operations, investigations and prosecutions.<sup>104</sup> Among these was the third annual exercise of Capstone's joint operations in East Africa, a preparatory agreement for one-month emergency preparedness in Kenya for security personnel from Kenya, Tanzania and Uganda.<sup>105</sup>

### **3.2.5 National Strategy to Countering Violent Extremism (NSCVE)**

Kenya embraced the National Strategy to Countering Violent Extremism (NSCVE) in 2016.<sup>106</sup> This strategy while focusing on the traditional terrorist threats is relevant to cyber terrorism. The comprehension behind the 2016 national approach that terrorism is similar to

---

<sup>103</sup> Bureau of Counterterrorism and Countering Violent Extremism. Country Reports on Terrorism 2016. Retrieved on 23 December 2018 from <https://www.state.gov/j/ct/rls/crt/2016/272229.htm>

<sup>104</sup> Beth Elise Whitaker, Reluctant Partners: Fighting Terrorism and Promoting Democracy in Kenya, *International Studies Perspectives* Vol. 9, No. 3 (August 2008), pp. 254-271

<sup>105</sup> Ibid

<sup>106</sup> <https://www.chrips.or.ke/publications/policy-brief/a-policy-content-evaluation-of-kenyas-national-strategy-to-counter-violent-extremism/>

many other national security risks is practically symptomatic of numerous different uncertainties that people or group(s) of individuals inside the nation could be confronting. The National Counter Terrorism Center (NCTC) is at the focal point of the usage of the strategy by enrolling and continuing the help of various government Ministries, Departments and Agencies (MDAs) in the battle against terrorism. NCTC has been instrumental in de-radicalization and reintegration of those that have separated from terrorism or violent extremism into the general public. Some portion of the technique included devolving the plans to counties in support the national CVE activity plans.

The Kenyan government in partnership with global players is focusing on CVE, the fight against radicalization and reintegration of returnees. The government proceeded with some success to restore and reinstate al-Shabaab's former warriors and facilitators, as it was hampered by a lack of facilities and a clear message.

In 2018, the NCTC began working with the Kenyan Ministry of Education on a school program to counter violent extremism. The same year, Kenyan security experts pointed out that Kenya's military strategy had led to a general decline in al-Shabab's violent activities, but online radicalization increased. In September 2018, the Center for Human Rights and Political Studies (CHRIPS) and the Institute for Development Studies jointly launched the Research Center to Combat Violent Extremism, an online library to support CVE research.

### **3.2.6 Private Sector**

The private sector in Kenya leads in automation of their systems. This makes it more susceptible to possible cyber-attacks including cyber terrorism on its critical infrastructure.

Thus, the sector can be influential including being resourceful in countering terror.<sup>107</sup> Strong infrastructures, such as financial institutions<sup>108</sup> and technological innovations, often help extremist operations.<sup>109</sup> However, terrorists also point to critical infrastructures in the private sector, such as banks, production, transport, telecommunications and health, with consequent asset losses and higher activity costs. This lays the foundation for the private sector's contribution to the fight against terrorism and mobilizing resources for corporate social responsibility programs for the benefit of affected communities or those at risk of radicalization. With the Internet being run by private sector players, the critical role they play in interdicting cyber-attacks that are ideologically inclined has gained momentum.

### **3.3 Multi Agency Counter Terrorism Strategies and Institutional Capacity**

The Government of Kenya has formed multi-agency teams to counter terrorism. The interagency coordination has led to improved information sharing.<sup>110</sup> However, it faces challenges in resources and training, command and control and operational matters.<sup>111</sup>

### **3.4 Counter Terrorism Financing**

Eastern and Southern Africa (ESAAMLG), a Financial Action Task Force (FATF-style) regional agency, has played a key role in combating money laundering. The mandate includes co-ordination with other international organizations involved in anti-money laundering, the

---

<sup>107</sup> Neal, S., Business as Usual? Leveraging the Private Sector to Combat Terrorism. *Perspectives On Terrorism*, 2(3). (2010). Retrieved 23 December 2018 from <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/31/html>

<sup>108</sup> Business-standard., *Kenya cracks down on financial firms over terror links*. (2016). Retrieved 23 December 2018, from [http://www.business-standard.com/article/news-ians/kenya-cracks-down-on-financial-firms-over-terror-links-115040800973\\_1.html](http://www.business-standard.com/article/news-ians/kenya-cracks-down-on-financial-firms-over-terror-links-115040800973_1.html)

<sup>109</sup> The Christian Science Monitor., *New encryption technology is aiding terrorists, intelligence director says*. (2016). Retrieved 23 December 2018, from [http://www.csmonitor.com/USA/Politics/monitor\\_breakfast/2016/0425/Newencryption-technology-is-aiding-terrorists-intelligence-director-says](http://www.csmonitor.com/USA/Politics/monitor_breakfast/2016/0425/Newencryption-technology-is-aiding-terrorists-intelligence-director-says)

<sup>110</sup> <http://lc.org/PDFs/StateDeptReportonTerrosirms2016COMPRESSED.pdf>

<sup>111</sup> Ibid

study of regional typologies in development, the development of institutional capacities and human resources to address these problems and the coordination of technical assistance where necessary. ESAAMLG allows regional factors to be taken into account when implementing measures to combat money laundering.<sup>112</sup>

Kenya's Financial Reporting Centre (FRC) is useful in monitoring financial transactions that are used to fund terrorist activities. Although the Central Bank of Kenya continues to encourage the use of the formal financial sector, the use of unregulated financial mechanisms, including hawala continues.

### **3.5 National, Regional and International Cooperation**

The International Telecommunication Union (ITU), in its Global Cybersecurity index of 2017, ranked third among the preparations to combat cybercrime and give the country a high score for its legislative framework and its technical capacity to respond to cybercrime incidents.<sup>113</sup>

Kenya has the National Coordination Center of the Kenya Computer Response Team (National KECIRT / CC) whose mandate is to monitor the cyber domain for any illegal activities. At national level this includes ISPs and the financial and education sectors; at regional level, it partners with the East African Communications Organization (EACO); at international level it is connected to the ITU, the Forum for the response to accidents and safety equipment (FIRST) and bilateral with the CIRT of the United States and Japan, among others.

---

<sup>112</sup> [https://suissebank.com/sites/default/files/SB\\_Application\\_Form\\_SBLC\\_EN.pdf](https://suissebank.com/sites/default/files/SB_Application_Form_SBLC_EN.pdf)

<sup>113</sup> ITU, Global Cybersecurity Index (GCI) 2017



### 3.6 Cyber Security Measures and Strategies in the Kenyan Perspective

The Internet was first introduced in Kenya in 1993, and its full use came into being in 1995. Formnet's first commercial application for the Internet service provider came into force in 1995, and many other Internet service providers entered the broadband Internet market, transformed as a result of increased investments in the digital network.<sup>114</sup> The expansion has enhanced broadband services which have been made affordable for the market. In the year 2000, Kenya had an inventory of nearly 200,000 Internet users with an assessed monthly growth at the rate of 300 new subscribers.<sup>115</sup> The main users of the Internet are Multinational Corporations, International Organizations, Non-Governmental Organizations (NGOs), government ministries and individual groups. In 2017, the Internet users in Kenya as per International Telecommunication Union (ITU) were estimated to be 43,329,434 people, translating to a penetration rate of 89.4 percent.<sup>116</sup> Among the achievements is the establishment of the Kenya National Cyber Security Master Plan 2017 and 2018, response centres and enacted laws to secure the ICT infrastructure against emerging threats.

A number of companies in ICT sector have invested in the business such as Nation TV (NTV), Kenya Data Networks (KDN), Safaricom (IGO Wireless), Telekom Kenya or (Orange Kenya), Internet Solutions Kenya (Inter Connect), MTN Business Kenya (UUNet), Jamii Telecom, Simba Net, Africa Online, Access Kenya (Dimension Data), Wananchi Online, Swift Global, Gilat Satellite Networks, Afsat Communications, Inmarsat, Indigo Telecom (Thuraya), KenTV, Liquid Telecom amongst others. This investment has enabled a

---

<sup>114</sup> Communications Authority of Kenya. (2015). First quarter sector statistics report for the financial year 2015/2016. <http://www.ca.go.ke/images/downloads/STATISTICS/Sector%20%20Statistics%20Report%20Q1%202015-16.pdf>.

<sup>115</sup> ITU, "Percentage of Individuals Using the Internet, 2000-2016,"

<sup>116</sup> Ibid

range of service provision such as video streaming, e-commerce, e-government and e-learning.<sup>117</sup>

The mobile penetration has increased from 89.2% to 90% according to the CAK report.<sup>118</sup>

The sustained growth in subscriptions of mobile phones has been enhanced by proliferation of affordable handsets and mobile data services including m-banking and m-commerce. According to Google Consumer Barometer survey, the number of Kenyans who use smartphone to access Internet services has increased tremendously from 27 per cent to 44 per cent in 2014 and 2016 respectfully.<sup>119</sup> This is because of the increased prominence in the use of internet platforms include access to Facebook, Twitter, WhatsApp and others. According to Nendo WhatsApp is assessed to have a population of about 10 million subscribers in Kenya.<sup>120</sup> WhatsApp has attracted more people as a channel for peers' conversation and interactions since the content shared on WhatsApp will be available on Facebook and Twitter.

In 2013, Kenya realized that ICT contributed about 12.1 percent of Kenya's GDP (Mwenesi 2014a).<sup>121</sup> These programme were largely supported by World Bank Group which invested around US\$4.1 billion for a number of years between 2010 and 2003 (Mwenesi 2014b).<sup>122</sup>

The Kenya Cyber Security Policy is presently coordinated by Communication Authority of Kenya.<sup>123</sup> Key tenets of the policy are computer access training and awareness, cyber safeguards and policies ICT economic drivers, ICT Governance and Legal framework.

---

<sup>117</sup> Akamai, The State of the Internet, Q1 FY 2017, Accessed 02 January, 2018. 2017, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-connectivity-report.pdf>.

<sup>118</sup> David Souter and Monica Kerretts-Makau, Internet Governance in Kenya – An Assessment for the Internet Society, Internet Society, September 2012.

<sup>119</sup> CAK: Q2 of the Financial Year 2016/2017.

<sup>120</sup>The *Nendo report*. 201411 highlighted the rise and growing power of Social Media influencers.

<sup>121</sup> Mwenesi, S. 2014a. ICT Contribution to Kenya's GDP now at 12.1%.

<sup>122</sup> Ibid.

<sup>123</sup> Paula, K., Carol, M., Kevin, K., Martin, M., & Barbara, S. (2014). Kenya Cyber Security Report 2014. Nairobi.

Through these strategies several teams have been established to oversee implementation of cyber technology and security measures as anchored in the law. Recognizing the importance of ICT, the Office of the Director of Public Prosecution (ODPP) has a branch devoted to cyber security crimes under the law.<sup>124</sup>

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. In December 2014, the country was witness to intrusion into its cybernetic space by foreigners from Thailand and China, arrested in Nairobi being in possession of equipment allegedly used to hack the ICT network. The group intended to hack Safaricom M-Pesa (mobile money transfer system), including ATM.<sup>125</sup>

Cybercrime in Kenya is estimated to cost over 175 million dollars and is likely to continue growing as more institutions automate their processes.<sup>126</sup> This is mostly 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>127</sup> The e-commerce for instance has been susceptible to serious online scams such as ATM card skimming and identity theft by unsuspecting cybercriminals.<sup>128</sup>

Despite these challenges, Kenya leads in mobile money business in Africa and other parts of the world. It records at least 27 Billion dollars in mobile money transfers annually. This growth has led to new and emerging threats that include malware attacks, fraud, stalking and phishing. The use of unsilenced software poses a security risk to users of mobile

---

<sup>124</sup> CAK (2015). Q1 sector statistics report for the financial year 2015/2016.

<sup>125</sup> Otuki, N. 2014. Beijing Says Runda Fraud Ring Likely Targeted China.

<sup>126</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>127</sup> Ibid

<sup>128</sup> Maina (2010), A survey on impact of ICT on Business Value Creation in Kenya Banking Sector. Unpublished MBA project, University of Nairobi.

application.<sup>129</sup> Kenyan banks are attractive to cyber criminals because of the vulnerable web applications and the platforms they use for financial transactions.

Kenya has continued to experience several mobile money thefts perpetuate through malware attacks and personifications of account. As banks embrace e-finance services, hackers are busy fighting to exploit weaknesses in mobile money security controls with an aim to steal. 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>130</sup>

Owing to this challenge, Kenya has gone ahead to develop strategies to respond to the rising cyber security threats by adapting to internationally recognized standards. Recognizing the importance of ICT in economic development, Kenya has chosen to seek partnerships with actors in the digital world to develop a strategy based on their experiences on the risks. With the support of the International Telecommunication Division (ITU), in 2012, the government set up a body called the National Coordination Center for Response to Cyber Security (KE-CIRT / CC) in Kenya to provide technical services for cybersecurity management. In accordance with the requirements of the Global Cyber Security Agenda, KECIRT / CC is responsible for providing advisory roles in national cyber security and cyber security reporting in co-operation with stakeholders at regional and international level. However, the center does not have the necessary skills, and it also lacks sufficient resources for full interaction with partners so it can lose importance in the industry.<sup>131</sup>

According to Business Daily (2013), 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

---

<sup>129</sup> Ibid, (2015).

<sup>130</sup> Seniuru, (2016).

<sup>131</sup> Kigen, et al, 2014. Kenya Cybersecurity Report 2014. [www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf](http://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf).

users. The absence of a devoted cyber security regulatory and legal framework places the country at a crossroad. The phenomenon of computer associated crimes is well known in the country and the growing international connectivity is likely to have serious consequences (UNODC, 2013).<sup>132</sup> Kenya acknowledges the Budapest Convention and Commonwealth Model Law on cybercrimes even though not a signatory to the convention (Global Project on Cybercrime, 2013).<sup>133</sup> Whereas, Kenya enacted a law on cybersecurity “Information and Communications Act 2009, according to this report, the legislations are not adequate to address the challenges of computer crimes”.<sup>134</sup> It is notable that Kenya lacks sufficient legislative policy and administrative framework to compel institutions as well as individuals to secure and protect personal data.<sup>135</sup>

Recognizing the challenges posed by the dynamic nature of ICT, Kenya has developed strategies to secure cyber security at the national level to ensure economic development and protect the interests of people. While charting its future, the government has identified numerous key concerns from the emerging risks from within and outside the borders from EAC, and internationally. For example, by providing a suitable environment for people to access and exchange information will enhance their reach in social life and business connections worldwide.<sup>136</sup>

The Kenya National Cyber Security Master Plan 2017/2018, is a strategy document that has been developed to address the risks that ICT is likely to face in future. The Strategy is built on the three pillars of Vision 2030 which define Kenya’s cybersecurity and objectives to be achieved in order to secure a safe cyberspace, while promoting ICT to an enabler to economic

---

<sup>132</sup> UNODC, World Drug Report 2013 (United Nations publication, Sales No. E.13.XI.6).

<sup>133</sup> Commonwealth Model Law, ITU Model Laws.

<sup>134</sup> UNODC Comprehensive Study on Cybercrime, 2013.

<sup>135</sup> Constitutional implementation in Kenya, 2010-2015: Challenges and prospects, FES Kenya Occasional Paper, No. 5 ISBN: 9966-957-20-0.

<sup>136</sup> The East African, *Kenya Launches Centre to fight cybercrime*, (2016).

growth. This is achieved through the adoption of the Kenya Information and Communications Act (KIC), Chapter 411A, which is an amendment to ICT Act 2014, and establishes the structure of a national certification body which aims to provide a framework for the implementation of public key infrastructure and partnerships with regional and international bodies to protect against cyber security. , It includes forums such as ITU and East African Telecommunication Organization (EACO).<sup>137</sup> The strategy will assist in making Kenya improve the current cybersecurity posture and provide guidance on how to secure cyber infrastructure against emerging threats. This will only be if there exists a strong cybersecurity doctrine reinforced with policy, legal and regulatory framework.<sup>138</sup>

In addition, 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. The center is established under CAK and is intended to respond to any online attacks or threats to security in the country.<sup>139</sup> In addition, the Computer and Cybercrimes Bill of 2016 which sought to align the law to developing forensic procedures when investigating increasing cases of cybercrimes is yet to be actualized.

### **3.6.1 Legislative Framework**

According to the second edition of Global Cybersecurity Index report 2016, Kenya is ranked amongst the top three African countries committed to cyber security measures.<sup>140</sup> In the newly established Kenya Cyber Security Policy 2016, all cyber threats are coordinated by the Communication Authority of Kenya. Key tenets of the policy are computer access training and awareness, cyber safeguards and policies ICT economic drivers, ICT Governance and

---

<sup>137</sup>Gagliardone, I., & Sambuli, N. (2015). *Cyber Security and Cyber Resilience in East Africa*. Centre for International Governance Innovation.

<sup>138</sup>Fischer, Eric A. (2005), *Creating a National Framework for Cyber security: An Analysis of Issues and Options*, February 22, CRS Report for Congress, Order Code RL32777.

<sup>139</sup> The East African, *Kenya Launches Centre to fight cybercrime*, (2016).

<sup>140</sup> Global Cybersecurity Index (GCI) 2017.

Legal framework.<sup>141</sup> Through these strategies several committees have been formed to oversee implementation of cyber technology and security measures as anchored in the law. Recognizing the importance of ICT, the ODPP has a branch devoted to cyber security crimes under the law.

### **3.6.2 Cybersecurity Laws**

The Kenya Government has taken measures to promote cyber security by adopting a series of laws. This includes the Information and Communications Act in Kenya, PAC 411A, amended by the Kenya Communications and Information Act (Amendment) 2014, the Computer Fraud and Cybercrime Law of 2018<sup>142</sup>, the Kenya Communications Law (Amendment 411) and the Law on the prevention of money laundering, no. 9 of 2009. The government founded the Kenya Cyber Incident Response Team (KE-CIRT / CC) and created a National Certification Center to ensure the implementation of public key infrastructure and cooperation with regional and international agencies and information security forums, including the International Telecommunication Union (ITU) and the Eastern Partnership Communication Organization (EACO). Although these actions and initiatives help the Kenya government to develop its position in IT security, the state of affairs of the Kenyan government in the field of computer security is still relatively immature because of the increasing complexity and complexity of cyber threats.

Other information security policies and regulations that have been amended include the IT security regulation (2016) and the IT security and protection law (2016). The 2012 Kenya Terrorism Prevention Law, the Crime Law and the 2011 Money Laundering Act and the 2010 Law on Organized Crime Prevention provide a solid legal framework for prosecuting acts of

---

<sup>141</sup> ICTA (2013). Connected Kenya 2017. R, <http://www.ict.go.ke/docs/MasterPlan2017.pdf>.

<sup>142</sup> <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf>

terrorism. It is likely that these new bills will influence the old laws and improve the management of information security.

### **3.6.2.1 The Computer Misuse and Cyber Crimes Act 2018**

The law on the misuse of computers and cybercrime intends to provide a framework for the identification and neutralization of cybercrime.<sup>143</sup> The law establishes penalties for those who commit terrorist attacks using computers, computer systems or networks. It also provides an elaborate mechanism to administer and guarantee an infrastructure of critical information against possible cyber-attacks by assessing threats, vulnerabilities and risks. and the likelihood of a cyber-attack in all areas of critical infrastructure.

The law also sets the foundations for international co-operation in the criminal prosecution of cybercrime. A crime database was created, by which any person who has information on a real threat or a cyber-attack is legally obliged to submit it to the database within 24 hours after the incident. The enactment of the law on computer crimes and computer crimes of 2018 has strengthened the collaborative framework between multiple agencies, among other key facets that support the national IT security recovery capacity.<sup>144</sup>

### **3.6.2.2 ICT Act 2013**

Kenya Information Communication Amendment Act 2013 includes Data Protection Bill (2013); introduces Cybersecurity, e-Commerce & Broadcasting legislations. It aims at developing safe, secure and effective environment for the cyber space by promoting and facilitating efficient management of critical internet resources.<sup>145</sup>

### **3.6.2.3 Communications Authority of Kenya (CAK) Cybersecurity Regulations**

---

<sup>143</sup> *Kenya Gazette Supplement No. 60 (Acts No. 5)*. The Computer Misuse and Cybercrimes Act, 2018

<sup>144</sup> <https://ca.go.ke/industry/cyber-security/overview/>

<sup>145</sup> Kenya Information and Communications (Amendment) Act, (2013).



The regulations of 2016 are envisaged to develop a framework that will facilitate the investigation and prosecution of cyber technology crimes and offences. It also aims to facilitate electronic commerce and eliminate barriers to e-commerce and e-leadership. It seeks to define Offenses and Penalties in case of breaches.<sup>146</sup>

#### **3.6.2.4 National Cybersecurity Strategy 2017/18**

Its goal is to promote the commitment of the government of cyber security. The strategy includes the following goals: Improve cybersecurity to promote the ICT e-business environment and eliminate vulnerabilities. To build cybersecurity awareness in order to develop competent workforce to address cybersecurity needs. This will be realized through training and sensitization workshops and other forums. In order to enhance collaboration and information sharing among relevant stakeholders and this will be accomplished through the established regional organizations and stakeholder's meetings. To develop national ICT leadership to develop cybersecurity strategies and legal frameworks at all levels.

### **3.7 Cyber Measures Based on Various Sectors**

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

#### **3.7.1 Banking Sector in Kenya**

The Central Bank of Kenya (CBK) under Section 33(4) of the Banking Act, has issued cyber security guidelines that will help banks deal with cybercrimes and prepare for emerging threats. These outline basic requirements institutions must take to protect against cyber-attacks. The guide helps create a secure and safe cyber space that is the foundation of

---

<sup>146</sup>Section 3, Draft Cybercrime Bill of Kenya (2014).

information security in the Kenyan banking sector. It places responsibility for protection of the institutions business to the line managers. It encourages all staff to implement IT security awareness training programmes and guide on best practice performance.<sup>147</sup>The Information Communication Technology Association of Kenya (ICTAK) has also offered to assist banks strengthen this regulation in order to combat cybercrimes.

In August 2018, the CBK issued Cyber Security Guidelines for Payment Service Providers (PSPs) in accordance with Section 31 (2) (b) of the National Payment System Act of 2011 authorizing the Central Bank to issue guidelines and guidelines to be to comply with payment service providers in order to maintain a reliable, secure and efficient national payment system.<sup>148</sup> The Guide describes the minimum requirements the PSP needs to develop in designing and implementing appropriate strategies, policies, procedures and activities aimed at reducing cyber-risk. The guideline is to create a safer and secure cyber space, which lies at the heart of security information system priorities, in order to promote the stability of the Kenya pay system subsector; to establish a coherent approach to preventing and fighting cybercrime; increasing the identification and protection of Critical Information Infrastructure (CII); promote compliance with relevant technical and operational standards of cyber security. The leadership of the PSP is focused on developing the skills required, continuously strengthening the capacity and culture of encouraging close interaction among politicians, using business technology and risk management; and help maintain public confidence in the national payment system.<sup>149</sup>

---

<sup>147</sup> Central Bank of Kenya Guidance Note on Cybersecurity, 2017.

<sup>148</sup> Central Bank of Kenya Guidance Note on Cybersecurity, 2017.

<sup>149</sup> Ibid

### **3.7.2 Mobile Service Providers (Safaricom)**

Safaricom maintains a modern information system (IT) security that automatically triggers a warning when detecting violations. The company has more than 17 million cyber security threats per day. The company managed to monitor cybercriminals through partnerships with CAK, National Police Service (NPS), National Intelligence Service (NIS) and other international networks such as Vodafone, providing information on potential threats in real time and responding to other threats cyber technology. come from other countries. Through a sustained surveillance and a multiple layers defence system through a chain of command that involves the maker, checker and authorizer of the system, Safaricom has been able to easily track any breaches.<sup>150</sup> Safaricom holds the world acclaimed ISO 27001 Information Security Management System Certification which confirms adherence to appropriate processes and controls in the industry.<sup>151</sup>

### **3.7.3 Academic Sector**

The Kenya Educational Network (KENET) is engaged in research and education supported by educational institutions. It provides affordable internet bandwidth to learning institutions. The learning institutions play an important role in strengthening IT security by participating in research and development (R & D). Kenya is lagging behind in R & D investments, leading to low innovations and the implementation of cutting-edge technologies. This trend could change if the Kenyan government collaborated with the institutions to develop

---

<sup>150</sup>Biztech Africa. (2011, October 29). Safaricom unveils cloud deployment. Available in <http://www.biztechafrika.com/section/internet/article/safaricom-unveils-largestnative-cloud-deployment-/1365/>.

<sup>151</sup> Kemibaro, M. (2011, October). Safaricom CLOUD: Safaricom's third act to dominate Kenya's telecoms sector?

appropriate technologies that could be implemented to ensure the critical infrastructure of public and private systems against cyber-attacks.<sup>152</sup>

### **3.8 Chapter Summary**

This chapter concludes that counter cyber terrorism strategies employed in Kenya have not fully matured. There are a number of disparate legislations and Acts of parliament that have been passed which would naturally have been collapsed into one legislative framework. While Kenya has developed cybersecurity measures and strategies, including legal frameworks, as an important step towards creating a secure environment for people and businesses, cybercrime continues to show resilience to strikes every day. Since the provision of these laws is meant to effectively deter cyber-crime, it is still a work in progress.

The next chapter provides a critical analysis of the effects of cyber terrorism on national security of Kenya.

---

<sup>152</sup>Bandara, I. Ioras, K. Maher, C. Lusuardi - Cyber Security Challenges of Distributed E-Learning Systems, 2015.

## CHAPTER FOUR

### THE CRITICAL ANALYSIS OF EFFECTS OF CYBER TERRORISM ON NATIONAL SECURITY IN KENYA

#### 4.1 Introduction

In the previous chapter, strategies were explored by the Kenya government to combat cyberterrorism with varying degrees of success. This chapter critically analyzes the impact of cyberterrorism on Kenya's national security. The chapter presents the results of the study. Data analysis was performed for each specific purpose. The data analysis is based on respondents' responses and is conducted using the Statistical Package for Social Sciences (SPSS), Survey and Microsoft Excel toolkit. The study used questionnaires to get the data. The questionnaire was sent either personally or online through Lime Survey.

#### 4.2 The Response Rate

In total, 37 questionnaires were distributed in this study, and respondents answered 29 questionnaires. This corresponds to the response level of 78.4%, sufficient for analysis, since it exceeds the 50% threshold proposed by Mugenda and Mugenda (2003).<sup>153</sup>

#### 4.3 Demographic Information

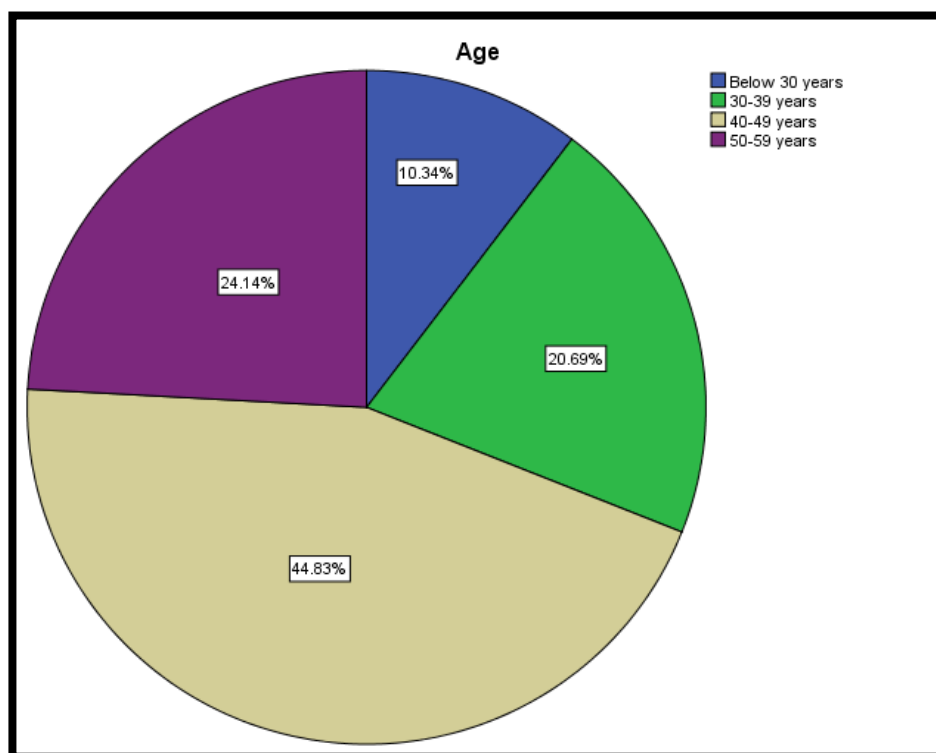
The researcher obtained demographic data in terms of sex, age, occupation, organization, experience and level of education. It was critical to know the demographic distribution of the respondents as it determines the effectiveness of the sample population.

---

<sup>153</sup> Mugenda, O.M., & Mugenda, A.G. (2010). Research methods qualitative & quantitative approaches. Nairobi: African Centre for Technology Studies

### 4.3.1 Age Distribution

Age was given as a range which accorded the respondents the opportunity to provide an accurate grouping for their ages. The answers are shown in Figure 1 below. According to the study, 44.83% of respondents were between the ages of 40 and 49; 20.69% at the age of 30 to 39; 24.14% were between the ages of 50 and 59, while 10.34% were under the age of 30.



*Figure 1: Age*

Most of the respondents are above 30 years an indication that they are working class people who may have interacted with technology, cyber threats and its effects.

### 4.3.2 Organisation Distribution

The study population covered the following; KDF, NIS Ministry of Interior, NCTC, ICT Authority (ICTA), National Police Service (NPS), Kenya Prisons Service, University, Private Sector and Ministry of Foreign Affairs. These organisations were specifically chosen because they are stakeholders in the security sector and had valuable information concerning cyberterrorism.

### 4.3.3 Work Experience

The respondents were asked how long they have worked for their respective organisations. Figure 2 below shows the level of experience gathered. 27.59% have over 20 hyears of service, 6.9% between 16 and 20 years, 17.24% 11 to 15 years, 31.03% 5 to 10 years and 17.24% below 5 years respectively. The respondents were well experienced in their fields and therefore are critical in strategy formulation and implementation. Their experience was quite useful in understanding the dynamics of technology and cyberterrorism.

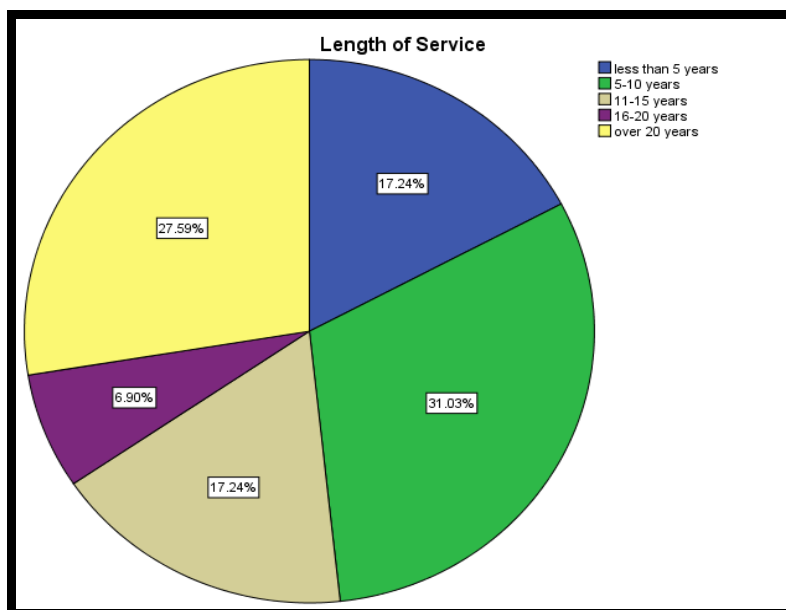
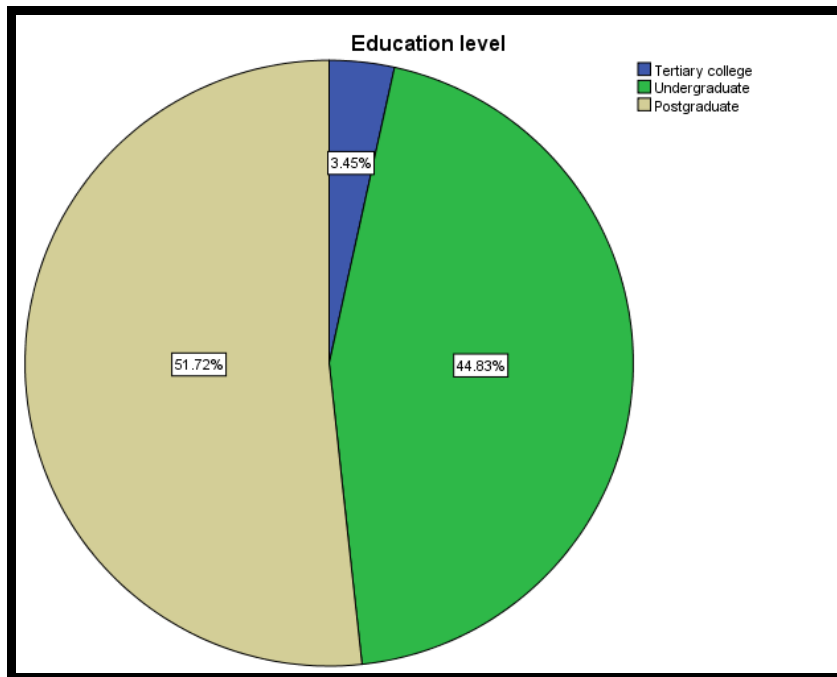


Figure 2: Length of Service

#### 4.3.4 Education Level

Figure 3 below indicates that 51.72% of the respondents had postgraduate degrees; 44.83% undergraduate; 3.45% tertiary education while none had secondary education.



*Figure 3: Education Level*

The implementation of strategies to counter cyber-terrorism needs experts. This study indicated that most respondents had ICT and security experience with over ten years of experience.

#### 4.4 Nature and Status of Strategies to Counter Cyber Terrorism

The study's first objective was to identify the nature and status of strategies used to fight cyber terrorism. Respondents were asked questions on cybercrime, incidents, causes and elements of cyber terrorism respectively.



The government of Kenya has established measures to counter cyber-terrorism. These include legislation on cybercrime, anti-money laundering laws, and anti-terrorism legislation among others.

#### **4.5 Cyber Crime and Cyber Attacks in Kenya**

Cybercrime is a crime that is approved or committed by a computer, network or hardware device. A computer or device can be an agent, agent or object of crime. Cybercrime can use violence that causes physical harm to people. They include cyber-terrorism, cyber-stem, bullying and pornography. Nonviolent computer crimes do not physically harm people. Instead, they cause financial losses, mental disorders, and social losses. The results of this study show that all respondents heard about cybercrime. This shows that the level of knowledge about cybercrime is very high.

The study identified a number of cybercrimes prevalent in Africa, especially Kenya. These cybercrimes include cyber-attacks that manifest terrorist elements. Data theft and corruption lead to sabotage of services, which is the most common form of Internet attacks. Table 2 below lists the various cybercrimes which shows financial/cyber fraud leading at 18% followed by hacking and identity theft at 13% and then by phishing and cyber stalking/bullying at 9% respectively.

While financial institutions do recognise the seriousness of fraud and attacks targeting banking systems, the deterrence strategy has not been well deployed. Most of the banks have been reactive than being proactive to cyber-attacks. The rise in hacking and identity theft is an indication that users are being targeted for their personal information which eventually is used to access financial records. Thus, identity theft becomes a facilitator to other cybercrimes.

Cyber terrorism is at 4% an indication that incidences of cyber terrorism attacks are still very low. Therefore, there no evidence to suggest that al-Shabaab has acquired the technology to implement a cyber or electronic attack. It is not known that the group performed one in the past, even though it was directed to telecommunications equipment. On 11 May 2018, militants destroyed a telecommunications pole in the area of Amuma, near the border with Somalia, while carrying out an attack in the town of El-Wak. And in December 2016, the militants destroyed four telecommunications trees belonging to the mobile companies Safaricom and Orange, in the county of Mandera in just one week.<sup>154</sup> The measure has blocked the region from the rest of the country for months and has left local residents for fear that militants will isolate them to carry out prolonged attacks.

In order to counter the threats of cybercrime, the government has adopted the Law on Computer Misuse and Cybercrimes (2018), which outlines the mechanisms for addressing cybercrime incidents. It also provides penalties and sanctions for any data breaches that may occur. The challenge is lack of information on cybercrime and attacks especially from the private sector more so the financial institutions. These institutions fear bad publicity which may result from exposure of their vulnerabilities making them opt to hide cyber-attacks and fraud from the public.

---

<sup>154</sup><http://www.nation.co.ke/counties/mandera/Shabaab-attack-again-Mandera/1183298-3484586-format-xhtml-144hmmu/index.html>

<b>Cyber Crime</b>	<b>Frequency</b>	<b>Percent</b>
Identity Theft	15	13%
Cyber Stalking/Bullying	10	9%
Child Pornography	5	4%
Social engineering	4	4%
Data Breaches	5	4%
Web Attack	8	7%
Phishing	10	9%
Cyber Terrorism	4	4%
DDOS/DOS	6	5%
Hacking	15	13%
Financial/Cyber Fraud	20	18%
Malware	6	5%
Ransomware	5	4%
Total	113	100%

*Table 2: List of Crimes*

#### **4.5.1 Ransomware**

Ransomware which is reported by about 4% of the respondents is attributed to the WannaCry ransomware which targeted a variety of organizations and institutions worldwide in 2017. The ransom note, written in several languages, required 300,000 US dollars from the victims to decipher their files. Cases of infection have been detected worldwide where several medical institutions have been affected, Russia, where government offices, Spain, Germany, China and many others have been affected.

Communication Authority's Kenya Computer Incident Response Team (KE-CIRT) reported that 19 Kenyan firms had been hit by the WannaCry ransomware. A number of firms were reported to have paid the requested ransom of \$300. These attacks succeeded because the organisations failed to implement a defence in depth strategy. The systems were weak and could not prevent an attack because of the inherent vulnerabilities. Effective protection against ransomware attacks requires the creation of backup copies that are resistant to the destruction of critical systems and data.

#### **4.5.2 Cyber Attacks on Digital Financial Services**

Low income earners have borne the brunt of cybercrime targeting digital financial services (DFS). Such acts if perpetrated by states or non-state actors with the intention of causing disaffection against financial system would greatly undermine the financial sector. Unfortunately, cyber-crime is a mounting issue in developing countries, including Kenya, where people use insecure phones to make financial transactions.

Kenyan banks have suffered intrusions or intrusions into their IT systems that have involved malicious software (malware), phishing, pharming and botnets or zombies. In July, 2018, Kenyan banks lost at least Kshs. 89 million to hackers. On January 17, 2018, National Bank of Kenya (NBK) confirmed that the institution had been hacked and at least Sh 29million had been lost in the incident. These attacks create serious credibility and reputation issues in the minds of the public on such instances. It also undermines the financial sector.

### 4.5.3 Social Engineering

In a social engineering attack,<sup>155</sup> victims are lured into revealing confidential and personal information or downloading malware which is used to hack into their systems or networks. It exploits people's trust in each other. DFS service providers in Kenya and other African countries, such as Ghana, Tanzania, Uganda and Zambia, have found that fraudsters force their employees to share information about their users and thus gain access to corporate information systems.<sup>156</sup> Most DFS distributors believe that negligent or unconscious employees are an important factor that puts their organization at cyber risk. But DFS clients are also vulnerable. New banking organizations are more likely to become victims of this program because of limited experience with digital fraud.<sup>157</sup>

By using social engineering approach, cyber terrorists would leverage on cybercrime tactics to lure gullible employees into revealing personally identifiable information that provide easy access to corporate networks. Suppliers can be protected from social engineering through regular information and training campaigns.

### 4.5.4 Data Breaches

Data violations are reported and the main problem is the database vulnerability. Hackers have been able to access data records such as credit card numbers, customer identification numbers, login credentials, and government identification data. Administering weak patches<sup>158</sup>, obsolete systems, and poor monitoring system monitoring are the main reasons why systems are susceptible to hacking attacks. In addition to financial losses that may arise due to data leakage, the reputation of the supplier and customer confidence has been

---

<sup>155</sup> <https://gomedici.com/social-engineering-elusive-adversary-cybersecurity/>

<sup>156</sup> "Nidhi Prabhu, Social Engineering: The Elusive Adversary in Cybersecurity, September, 2018"

<sup>157</sup> Ibid

<sup>158</sup> <https://www.ncsc.gov.uk/topics/patch-management>

compromised. To protect data leakage, it is necessary to periodically update systems, remove vulnerabilities, and install software patches. You may also need to apply advanced encryption for inactive and transit data and monitor the 24/7 registry.

#### **4.5.5 System Outages and Denial of Service Attacks**

In December, 2018, Safaricom Mpesa<sup>159</sup> experienced a five hour outage that affected financial transactions in the entire country. M-Shwari's clients also faced a similar attack.<sup>160</sup> Most systems have experienced denial of service. With denial of service attack, cyber criminals fill the server with simultaneous access requirements, allowing legitimate users to disable access to the system.

Monitoring of the network traffic and detecting any anomalies would be a first level of protection. Then once any anomaly is detected, its resolution is immediately undertaken through appropriate restore procedures.

#### **4.6 Causes of Cyber terrorism**

According to game theory<sup>161</sup>, cyber terrorists like to commit malicious acts when they believe this will help to influence decision makers directly on cyber-terrorist goals.<sup>162</sup> The main goal of cyberterrorism is to damage the computer system.<sup>163</sup> This can be done by first ensuring

---

<sup>159</sup><https://techweez.com/2018/12/09/mpesa-service-outage/>

<sup>160</sup><https://www.businessdailyafrica.com/news/M-Shwari-downtime-persists-for-fifth-day/539546-4244684-lmdt8m/index.html>

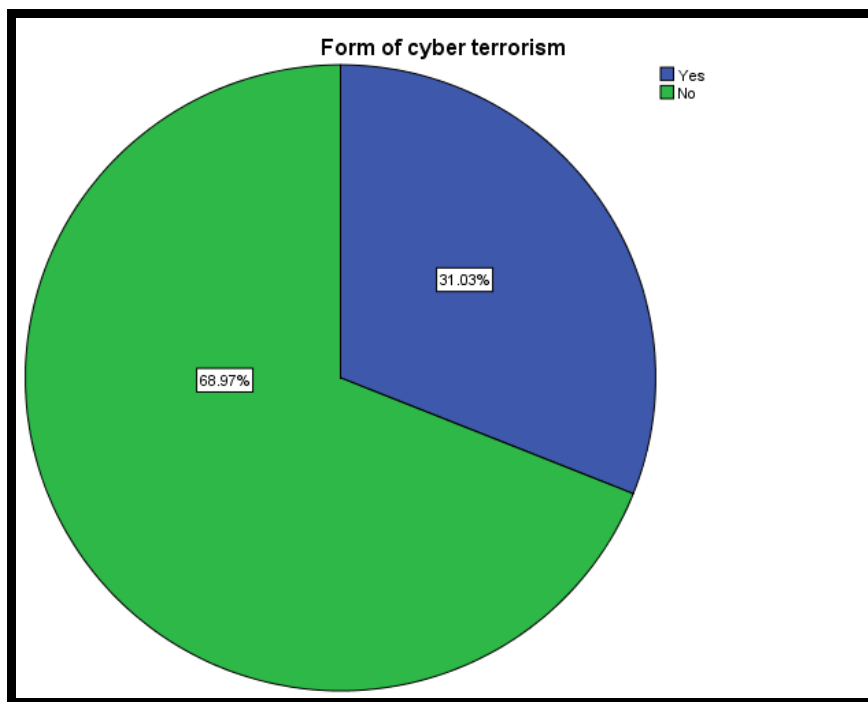
<sup>161</sup> Lye, K. W. and Wing, J. M. (2005). Game strategies in network security. *International Journal of Information Security*, 5(1), pp. 1–10.

<sup>162</sup> Matusitz, Jonathan(2009) A Postmodern Theory of Cyberterrorism: Game Theory, *Information Security Journal: A Global Perspective*, 18: pp. 6, 273 — 281

<sup>163</sup> Sallhammar, K., Helvik, B. E., and Knapskog, S. J. (2005). Incorporating attacker behavior in stochastic models of security. In *Proceedings of the 2005 International Conference on Security and Management*, Las Vegas, NV.

the system's security is enhanced. Second, any activity that causes damage to the systems is beneficial to terrorists.<sup>164</sup>

According to research findings, only 31.03% of respondents reported having experienced any form of cyber-attack or cyber terrorism while 68.97% have never experienced any attack as shown in figure 4. Some of the reported incidents include denial of service attacks in 2015, the bandwidth of vehicle inspection, which was flooded with data packets; access to internet sites of cyberterrorism; distortion of government websites, identity theft in networks and systems.



*Figure 4: Experience of Cyber Terrorism*

According to the respondents, the underlying causes of cyber terrorism include availability of software tools or cyber weapons that can easily conduct attacks on multiple systems and

---

<sup>164</sup> Ibid

networks, automation of critical infrastructure making them targets, insufficient security controls to automated systems. Religious fanaticism (emergence of cyber caliphate), political ideology and violent extremism were also identified as causes of cyber terrorism. The ubiquitous nature of advanced technology makes it easily amenable to attacks. A youth bulge dividend has not been adequately/effectively harnessed and therefore the youth being bored and want to be adventurous. Available information on radical teachings both on YouTube, social media sites and blogs as well as ungoverned space where criminals propagate radicalisation narratives.

#### **4.7 Strategies to Fight Cyber Terrorism in Kenya**

Terrorist organizations such as al-Qa'ida and the Islamic state can be effectively maintained.<sup>165</sup> To understand the strategies used to fight cyberterrorism in Kenya, an examination of the various entities involved was carried out. Respondents were asked to evaluate organizations involved in cyberterrorism with a very low degree = 1, low degree = 2, moderate degree = 3, high degree = 4 and very high degree = 5. 11 elements were estimated. The National Intelligence Service is very high - 51.7% followed by National Counter Terrorism Centre at 34.5% and Kenya Defence Forces at 27.6%.

In terms of measures that are used to curb cyber terrorism, the respondents rated twelve attributes. The multi-Agency approach to curbing cyber terrorism is rated very high at 69% with Legislation and capacity building and awareness following at 65.5% and 62.1% respectively. The study findings indicate that the strategies employed by the Government of Kenya involve multi-agencies, private sector and international partners. The participation of

---

<sup>165</sup>John J. Klein, *Deterring and Dissuading Cyberterrorism*, ASPJ Africa & Francophonie, 2018” ; “Gray, *National Security Dilemmas*, 2011, p. 72.



international partners leads at 26.33% followed by private sector at 25.33% and then multi-agencies at 24%.

According to the study, international partners are involved in funding, sharing information and intelligence on cyber terrorism suspects as well as dismantling online syndicates of terrorism. They also provide training and capacity building to the law enforcement personnel. The Computer Misuse and Cybercrimes Act (2018) provides a platform for government to engage with international partners on cybercrime issues such as extradition of persons suspected and accused of committing cybercrimes. By engaging international partners, the government benefits from the technical capacity and legal support required to investigate cyber terrorism.

The private sector especially the financial institutions who are greatly affected by cyber crimes, are liable for protecting their own IT systems and the government constantly engages with them to determine the level of preparedness against cyber-attacks and during attacks to help mitigate the effects of such attacks. For companies in the hospitality industry such as hotels, they are required to exercise care in scrutinizing identity documents, transaction documents, movement and behaviour patterns of their clients. The Kenya Private Sector Alliance (KEPSA) has been involved in a number of online forums to educate customers and their members on cyber issues. The private sector has been able to share data with government agencies on suspects involved in any terrorism related crime. This includes the mobile network operators and banks. The private sector is actively involved by constantly investing in tools, systems and processes that protect their business operating environments and by extension, their customers.

The Government of Kenya has employed a multi-agency approach to tackle the threat posed by cyber terrorists. According to the respondents, there is close collaboration between NIS,

KDF, Directorate of Criminal Investigations (DCI) and Communications Authority of Kenya (CAK) in the fight against cyber terrorism. At the same time, NCTC has been involved in online sensitisation through the citizen support portal on matters concerning terrorism, de-radicalization and terrorism financing among others. The coordinated approaches and efforts have been key in the gains witnessed in the fight against terrorism. The multi-agencies cooperation has assisted in sharing of timely information for action by different security agencies. The National Computer and Cyber Crime Coordination Committee membership as per the Computer Misuse and Cybercrimes Act (2018) reflects a multi-agency approach(through its membership). This was one of the most important aspects of Kenya's anti-terrorism strategy. The multisector approach to combating terrorism is more inclusive and includes non-security stakeholders from the government and the private sector. These relevant stakeholders emphasize soft power approach which is important for counter terrorism strategies. The government has engaged the Department of Commerce United States of America and Local US Embassy in Kenya in training law enforcement agencies on how to counter cyber terrorism.

An effective strategy would require application of cyber surveillance and monitoring; facilitation of information sharing among security/intelligence services; regional collaboration and sharing of information among African countries and engagement with the local communities to enhance a climate of trust and cooperation with the citizens. This strategy resonates with the overall cyber deterrence and prevention of cyberterrorism.

#### **4.8 Effects of Cyber Terrorism on National Security**

The implications of cyberterrorism are different, and respondents have responded to what particular phenomenon threatens Kenya's security and stability. According to the study,

online radicalization leads to 31%, followed by cybernetic attacks by 23%, followed by hacker attacks and denial of service attacks by 18%.

According to the respondents cyber terrorism has a very high impact on economic security, followed by military and then political and human security. All these factors deny the common citizen the basic rights as enshrined in the constitution of Kenya. Compromising economic security results in loss of funds especially large amounts for financial institutions. Economic, Human, Military and Politics are issues that are critical to the day to day running of a nation and so any cyber terrorist attack on either of the four elements is critical to national security matters of a nation. For the case of human security and politics they aver that cyber terrorism may manipulate information and compromise good governance and harmonious relations. In the case of military, it may affect operations, safety and military intelligence negatively. Therefore, cyber terrorism effect on economic, human, military and politics security of any country is very high because these are pillars of a nation. The respondents were of the view that cyber-attacks could defame a government and is a new frontier in radicalization as it conceals concerned parties and reaches wider audiences. They assert that cyber terrorism has led to spread of hate material, loss of income and even tribal animosity hence affecting people economically and socially.

However, they noted that the Government of Kenya has put in place certain measures to counter cyber terrorist attack. These include establishment of Computer Security Incident Response Centre (CSIRT), multi-agency counter terrorism strategy, legislation and establishment of Cyber Command Centre. The respondents also noted that the Computer Misuse and Cybercrimes Act (2018) is yet to be fully implemented. Meanwhile, the establishment of cyber command centres and CSIRT has enhanced response to cyber-attacks within government. Cyber Command Centres and CSIRT are key in coordinating the

receiving and responding to any cyber incidents while the multi-agency helps in sharing of timely information concerning an incident and the legislation helps in the prosecution of offenders. Previously, different government agencies fought terrorism separately. Multi-agency approach brings synergies of these agencies together and helps to fight cyber terrorism more effectively and efficiently.

According to the data obtained, cyber terrorism is a threat to national security. The threat is manifested against critical infrastructure such as railways, ports, airports, mobile networks, health services, energy services, communications/ICT networks, e-citizen, Huduma centre services, banking services etc.

#### **4.8.1 Effects of Cyber Terrorism on the Economy**

The study findings show that cyber terrorism may have a wider and far reaching impact on society based on the interconnectedness of the global village. The respondents identified financial and stock markets with over half indicating they have been subject of cyber-attack and online banking fraud. They attribute the susceptibility of financial institutions to cyber-attacks to the vulnerable electronic banking system. According to the respondents, MPESA transactions faced the highest level of attack and losses. A report from Safaricom indicates the company lost at least 20 million shillings through fraud.<sup>166</sup> However, they were not able to quantify the cost of cyber terrorism because many organisations shy from disclosing breaches of their systems.

According to the findings, the effect to the financial markets which is sensitive to any negative effects include breaches to financial data thus raising cost of doing business with some of the firms being considered high risk. The firms also fear reputation damage and loss

---

<sup>166</sup> <https://nairobinews.nation.co.ke/news/safaricom-lost-sh20-million-to-fraudsters-this-year>

of trust of its clients following disclosures of security breaches. Public disclosure of attacks may also leak information to hackers about the state of vulnerability of the firm.

For the stock market, the price of a company's shares is a consequence of the value that comes from its production. When a violation occurs, it affects both stock performance and revenue. Firms may be affected based on the level of exposure of their systems. Firms with physical locations of operation are less likely to suffer cyber-attacks compared to those operating online.

According to the respondents, the insurance industry has had to grapple with the need to cover cyber-attack losses. Previously, business reporting such losses was never compensated. The insurance industry has not been keen to introduce coverage for cyber threats. The study has shown that there is a legal gap in terms of covering cyber-attack losses.

#### **4.8.2 Effects of Cyber Terrorism on Human Security**

The respondents indicated that cyber terrorism has a direct impact on human security. When an attack occurs, nearly all the elements of human security are affected. For example, cyber-terrorism that results in denial of service would create apprehension and disorder among the population. Terrorists need domination, their training and the motivations they pursue differ, but they are united by the most common desire of death to induce fear in the target society.

#### **4.9 Chapter Summary**

This chapter discussed the implications of cyberterrorism for national security. However, the attacks that have been committed in Kenya are currently part of cybercrime. However, due to the vulnerabilities observed in most critical systems, there is a great fear that a cyber-attack

on critical infrastructure will have detrimental consequences for the economy, national security and human security.

The effects of cyberterrorism are more prevalent and can lead to losses. They target critical infrastructure, vulnerable systems and online systems. Beyond the threat cyber terrorism poses to military and security interests, lies the human dimension of cyber terrorism. In its extant nonlethal forms and its foreseeable lethal forms, cyberterrorism mirrors and, indeed, builds upon the psychological suffering endemic to kinetic terrorism.

The next chapter summarizes the results of the research and brings conclusions based on the hypothesis used to address three research questions. The chapter also provides recommendations and areas for further study.

## **CHAPTER FIVE**

### **SUMMARY, CONCLUSION AND RECOMMENDATION**

#### **5.1 Introduction**

This chapter summarizes the findings, conclusions and recommendations from the research project. The final part of the chapter contains suggestions for areas that require further study.

#### **5.2 Summary of Findings**

The study sought to promote security in Africa through effective strategies against cyber-terrorism using the Kenyan case study. While there is no evidence of a cyber terrorism attack on Kenya, several cyber-attacks have been reported. The study therefore identified nature and status of strategies in place, effects and counter cyber terrorism measures required to mitigate the threat.

##### **5.2.1 Nature and Status of Strategies and Infrastructure to fight Cyber Terrorism**

The study found the main underlying causes of cyber terrorism include availability of software tools or cyber weapons that can easily conduct attacks on multiple systems and networks; insufficient security controls to automated systems; religious fanaticism (emergence of cyber caliphate); political ideology and violent extremism. Other causes include failure to deal with youth bulge who get bored and want to be adventurous and also the relative ease with which people access information on radical teachings both on YouTube, social media sites and blogs as well as ungoverned space where criminals propagate radicalisation narratives.

The study also identified various elements influencing cyberterrorism. These include state sponsorship and non-state actors with criminal or illegal intent to use cyberspace for violence against people or property. The motive of attack may be political or ideological.

It should be noted that cyber criminals have a problem cleaning the proceeds from their fraudulent activities. It may involve a process of money laundering. Enhanced security measures implemented by financial institutions make cyber terrorism attacks rather remote.

Significant preparations that improve cyber resilience demonstrate that cyber-attack would not have the desired effects. Consequently, the adversary's leadership may refrain from pursuing a cyber-attack as the benefits may not be much or decide to follow another path of destruction.

This phenomenon explains Africa's crime rate associated with digital activities mainly in the social media as a clear pointer to an existing gap in the continent's digitalization programme.

### **5.2.2 Strategies to Fight Cyber Terrorism in Kenya**

The study found the strategies that have been employed to counter cyberterrorism include the multi-Agency approach; cyber legislation; capacity building and awareness. The study found out that the strategies involving multi-agencies; private sector and international partners are more effective compared to the rest.

Further, in terms of techniques, the study found out that an effective strategy would require application of cyber surveillance and monitoring; facilitation of information sharing among security/intelligence services; regional collaboration and sharing of information among African countries and engagement with the local communities to enhance a climate of trust



and cooperation with the citizens. This strategy resonates with the overall cyber deterrence and prevention of cyberterrorism.

While Kenya has developed cybernetic security measures and measures, including legal frameworks, as an important step towards creating a safe environment for people and businesses, cybercrime continues to show resistance to strikes on a daily basis. Since the provision of these laws is meant to effectively deter cyber-crime, it is still a work in progress.

Through the multi-agency approach, the country is ready and prepared to handle cyber-attacks that include cyber terrorism. Other key strategies include legislative framework that include the enactment of the Computer Misuse and Cybercrimes Act (2018) which provides the legal mechanism of dealing with cybercrimes including cyber terrorism.

Capacity building, training and awareness have are key determinants of the level of preparedness of the law enforcement personnel and the public about cyber-terrorism. Another approach involves collaboration with international partners. According to the study, international partners are involved in financing, exchanging information and intelligence on suspects on cyber-terrorism, as well as in the abolition of internet terrorism syndicates. They also provide training and capacity building to the law enforcement personnel.

The Kenya Private Sector Alliance (KEPSA) has been involved in a number of online forums to educate customers and their members on cyber issues. The private sector has been able to share data with government agencies on suspects involved in any terrorism related crime. This includes the mobile network operators and financial institutions.

The study also identified social media and the internet, NGOs and Civil Society groups, Kenya Community Support Centre, SUPKEM as key actors in the implementation of strategies to counter cyberterrorism.

### **5.2.3 Effects of Cyber Terrorism on National Security**

The study found a number of factors concerning cyberterrorism that impact national security. Among the factors, the main concern was online radicalisation, cyber-attacks and website defacement. In terms of effects on various security sectors, the study found out that cyber terrorism has a very high impact on economic security, followed by military and then political and human security. All these factors deny the common citizen the basic rights as enshrined in the constitution of Kenya. Compromising economic security results in loss of funds especially large amounts for financial institutions. Economic, human, military, and political issues are crucial to day-to-day activities of the nation, and therefore every cyber-terrorist attack on any of the four elements is crucial to the national security issues of the nation.. For the case of human security and politics it may manipulate information and compromise good governance and harmonious relations. For military, it may affect operations, safety and military intelligence negatively. Therefore, cyber terrorism effect on economic, human, military and politics security of any country is very high because these are pillars of a nation. Cyber terrorism can defame a government and is a new frontier in radicalization as it conceals concerned parties and reaches wider audiences. Cyber terrorism has led to spread of hate material, loss of income and even tribal animosity hence affecting people economically and socially.

The Kenya Government has taken certain measures to combat cyber-terrorist attacks. These include establishment of Computer Security Incident Response Centre (CSIRT), multi-agency counter terrorism strategy, legislation and establishment of Cyber Command Centre. However, Computer Misuse and Cybercrimes Act (2018) is yet to be fully implemented. The cyber command centres and CSIRT are critical units that organisations require to respond to cyber-attacks. Their establishment has enhanced response to cyber-attacks within

government. Cyber Command Centres and CSIRT are key in coordinating the receiving and responding to any cyber incidents while the multi-agency helps in sharing of timely information concerning an incident and the legislation helps in the prosecution of offenders. Previously, different government agencies fought terrorism separately. Multi-agency approach brings synergies of these agencies together and helps to fight cyber terrorism more effectively and efficiently.

According to the data obtained, cyber terrorism is a threat to national security. The threat is manifested against critical infrastructure such as railways, ports, airports, mobile networks, health services, energy services, communications/ICT networks, e-citizen, Huduma centre services, banking services etc.

### **5.3 Conclusion**

Cyberterrorism while having a low propensity for serious damage, based on non-availability of attack vectors to cyber terrorists, is still a threat to national security especially the critical infrastructure. This study sought to examine how security can be promoted in Africa through effective counter cyber *terrorism* strategies using the case study of Kenya. The findings presented in the previous chapter highlights the causes, incidents, elements, strategies and effects of cyberterrorism. The findings answer the broad research question on promoting security in Africa through effective cyberterrorism strategies.

The first chapter presents three research questions. First, what is the nature and state of strategy and infrastructure for fighting cyberterrorism in Africa? Second, what strategies are used to combat cyber terrorism in Kenya? Third, what are the common consequences of cybercrime for national security in Kenya? The research has attempted to answer these research questions with the following three hypotheses:

**Hypothesis I:** The failure to adopt effective cyber terrorism strategies has led to increased insecurity in Africa.

This hypothesis is based on the nature and status of strategies and infrastructure put in place to counter cyberterrorism in Africa. Various critical infrastructure components were identified and the strategies required protecting them highlighted. The strategies to counter cyberterrorism identified include cyber legislative framework, cyber deterrence and dissuasion, cyber defense, concession and retaliation.

The African Union, in a meeting held in Malabo on June 26 and 27, 2014, adopted the Convention on cyber security and the protection of personal data. It dealt with legislative problems arising from criminal activities in ICT networks in a compatible manner on a regional and continental level and in response to the need for harmonized legislation in the field of cyber security and the protection of personal data in African countries.

This is a manifestation of the seriousness with which the African Union is addressing cybersecurity issues. The AU went further and developed the following action points for national governments of member states: Development of national strategies for cyber security in accordance with international standards and practices; Support the creation of national cyber security management and define stakeholder roles and responsibilities; Development of the regulatory framework and special provisions related to cyber-legislation; Enhanced technical capacity for monitoring and protection of national networks; Development of National Computer Emergency/Incident Response Teams (CERTs / CIRTs); Encourage efficient sharing of information and digital evidence on bilateral or multilateral basis; Protect relevant Institutions and the integrity of critical National Infrastructures; Provide long term capacity building and technical assistance to strengthen the national authorities to deal with

cybersecurity issues; Designate a focal point to facilitate regional and international cooperation.

**Hypothesis II:** The adoption of relevant cyber terrorism strategies will reduce incidences of cyber terrorism in Kenya.

This hypothesis identified the various strategies adopted and implemented in Kenya. The main strategy is the enactment of the Computer Misuse and Cybercrimes Act(2018), cyber surveillance and monitoring; facilitation of information sharing among security/intelligence services; regional collaboration and sharing of information among African countries and engagement with the local communities to enhance a climate of trust and cooperation with the citizens.

**Hypothesis III:** The counter cyber terrorism strategies employed in Kenya apply a multi-agency approach.

This strategy applies the multi-agency approach that incorporates various stakeholders within the security sector, private sector and international partners. These hypotheses have been examined in the previous chapters based on how the objectives have been addressed. The hypotheses have been covered in chapters two, three and four respectively. For example, chapter two covered the nature and status strategies and infrastructure for countering cyberterrorism in Africa. The first hypothesis shows that the measures deployed fits in with the African Union mechanisms. Failure to adapt effective counter cyberterrorism strategies exposes the critical infrastructure to cyber-attacks including cyberterrorism.

The second hypothesis is the approach to the Law on Computer Misuse and Cybercrime (2018), as well as the creation of the National KE-CIRT-CC, which deals with cybercrime and cybercrime in the country. Some of the cybercrimes covered include cyber fraud, child

pornography, cyber espionage, phishing, interception and destruction of electronic messages, cyberterrorism, hacking, illegal access and interception.

The third hypothesis is congruent with the multi-agency approach the government has deployed to deal with cybersecurity and cyberterrorism related threats. A multi-agency approach was first applied to the fight against traditional terrorism. To effectively fight Al Shabaab, the government put together teams from the security agencies to undertake an operation to flush out the militants out of Boni forest in Lamu County.

The key conclusion of this study is that, cyber terrorism pose an insignificant threat to Kenya. Terrorists are more inclined to use the traditional methods than apply cyber tools because physical harm to citizens gives them publicity compared to bringing down a system.

Therefore, effective cyber terrorism strategies employed are adequate to promote security in Africa and especially Kenya if they are properly enforced. Maintaining cyber resilience will deter would be attackers from employing cyber weapons.

The research has shown that the nature of infrastructure is highly automated and counterterrorism strategies at regional and national level have the potential to deter cyber terrorists. However, more resilience and cyberspace surveillance is required to ensure the infrastructure is always secured.

Considering these together, the examination of Kenya's counter cyberterrorism strategies demonstrate that the hypotheses introduced in chapter one have been proven.

## 5.4 Recommendation

This research is used to produce new knowledge that will help in promoting security in Africa through effective counter cyber terrorism strategies particularly in Kenya. It is also used to enlighten the policy makers on the need to understand structural and operational performance of the cyberspace for better functioning of national cyber security systems. While Kenya has suffered conventional terrorism for some time, and has adopted measures to confront it, the possibility of a shift from conventional terrorism to cyber-terrorism presents a security gap. Finally, this study contributes to the existing academic literature on emerging trends and patterns of cyber terrorism, which could be useful to scholars and academicians dealing with the subject matters, especially given the ever expanding dynamism of cyber-attacks today.

These measures have included requisite legislative framework, multi-agency cooperation, protective security and defense-in-depth strategy. Among these measures deterrence and information or intelligence sharing takes precedence. The recommendations are:

### **Recommendation 1:** Prevent/Counter Violent Extremism and Radicalization

Implement surveillance and monitoring systems that enables the government to detect those being radicalized through social media platforms. This will also provide an avenue for interdicting possible recruitment and fundraising for terrorist networks. The social networking sites have become a training ground for terrorists. Since the youth have embraced technology, they have become target of terrorists who provide propaganda videos and manuals. Such surveillance systems would help security agencies identify sites that are used for radicalization. The system should be able to monitor terrorist communications and foil their plans before they occur. The system should be geared towards protecting the

infrastructure, enhance situational awareness and analysis, provide early warning and risk management.

**Recommendation 2:** Strategies to combat cyberterrorism

The government could ensure that the measures taken are a comprehensive and integrated counterterrorism strategy based on the United Nations Global Counter-Terrorism Strategy, which is a tool for improving national, regional and international efforts to combat terrorism. Furthermore, policy makers should have measures for countering terrorism financing.

**Recommendation 3:** Enhancing inter-agency collaboration and International cooperation

Having an inter-agency collaboration is an effective means of fighting cyberterrorism. However, the efforts in place should be enhanced to ensure the established of a national cyber command and control centre. This will provide a one-stop-shop for all matters concerning cybersecurity. The government must provide and improve support, professional connections between the competent organs against terrorism at global, regional and national level. Efforts should be made to improve cooperation in capacity building in the fight against terrorism.

It is important to ensure that the private sector plays a more effective role in integrating government efforts to combat cyber-terrorism. This is because the private sector has invested heavily in technology that would be severely impaired if a cyber terror attack was to take place. Second, enhance public participation so that law enforcement agencies get a forum to interact with the public whether online or physically as an opportunity to create awareness on the effects of cyber terrorism.



## **5.5 Suggestion for Further Studies**

The study sought to promote security in Africa through effective counter cyber terrorism strategies using the case study of Kenya. The study accomplished its objectives. However, because of the nature of cyber terrorism, there is need to undertake further study in the following areas:

1. Since the threat of cyber-terrorism in Africa is still small, it is necessary to extend the scope to include other jurisdictions, such as Europe and America, for comparative research.
2. A study to determine the cost implication of cyber terrorism and its impact on the economy.

## **Bibliography**

### **Journal Articles, Books and Documents:**

- African News. (2010b). Kenya: Banks Fight to Secure Customers Deposits from Cyber Criminals. Business Daily (Nairobi)
- Akamai, The State of the Internet, Q1 FY 2017, 2017, <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-connectivity-report.pdf>. Accessed on 12 February, 2018.
- Anthony G. Turner, Sampling frames and master samples. United Nations Secretariat, Expert Group Meeting to Review the Draft Handbook on Designing of Household Sample Surveys 3-5 December 2003
- Arcworld., Supreme Council of Kenya Muslims Strategic Plan and Transition from MDGS TO SDGS. (2015) Retrieved 23 December 2018, from <http://www.arcworld.org/downloads/SUPKEM.pdf>
- Article 51, Charter of the United Nations and Statute of the International Court of Justice (San Francisco, CA: United Nations, 1945), available at: <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>.
- Austin Long, Deterrence: From Cold War to Long War (Santa Monica: RAND, 2008), 5, [http://www.rand.org/pubs/monographs/2008/RAND\\_MG636.pdf](http://www.rand.org/pubs/monographs/2008/RAND_MG636.pdf).
- Bandara, I. Ioras, K. Maher, C. Lusuardi - Cyber Security Challenges of Distributed E-Learning Systems, 2015.
- Barabasi, A. L., & Bonabeau, E. (2003). Scale-free networks. *Scientific American*, pp. 288, 60-69.
- Bavelas, A. (1950). Communication patterns in task-oriented groups. *Journal of the Acoustical Society of America*, 22, pp. 725-730.
- Beccaria, C. (1963). *On crimes and punishments* (introduction by H. Paolucci, Trans.). New York: Macmillan. (Original work published 1764)
- Bentham, J. (1948). *An introduction to the principles of morals and legislation* (with an introduction by W. Harrison, Ed.). New York: Macmillan
- Beth Elise Whitaker “Reluctant Partners: Fighting Terrorism and Promoting Democracy in Kenya”, *International Studies Perspectives* Vol. 9, No. 3 (August 2008), pp. 254-271
- Biztech Africa. (2011, October 29). Safaricom unveils cloud deployment. Available in <http://www.biztechafrika.com/section/internet/article/safaricom-unveils-largestnative-cloud-deployment-/1365/>.
- Boey, Darren. North Korean Hacker Group Linked to Taiwan Bank Cyber Heist. *Bloomberg Technology*. (2017), p. 8-12.
- Boey, Darren. North Korean Hacker Group Linked to Taiwan Bank Cyber Heist. *Bloomberg Technology*. (2017), p. 8-12.
- Brenner, W. *Cybercrime: Criminal Threats from Cyber Space*. Santa Barbara, California: Greenwood Publishing Group, (2010), p. 38.

- Bureau of Counterterrorism and Countering Violent Extremism. Country Reports on Terrorism 2016. Retrieved on 23 December 2018 from <https://www.state.gov/j/ct/rls/crt/2016/272229.htm>
- Burgess, Matt. What is GDPR? WIRED explains what you need to know. Wired, (2018), p. 12-19.
- Business-standard., Kenya cracks down on financial firms over terror links. (2016). Retrieved 23 December 2018, from [http://www.business-standard.com/article/news-ians/kenya-cracks-down-on-financial-firms-over-terror-links-115040800973\\_1.html](http://www.business-standard.com/article/news-ians/kenya-cracks-down-on-financial-firms-over-terror-links-115040800973_1.html)
- Carrier, N. and Lochery, E. 2013. "Missing States? Somali Trade Networks and the Eastleigh Transformation." *Journal of Eastern African Studies* 7 (2).
- Central Bank of Kenya Governor Patrick Njoroge during the Monetary Policy Meeting in Nairobi held amid backdrop of improved weather conditions on May 30,2017.
- Central Bank of Kenya Guidance Note on Cybersecurity, 2017.
- Chairman, Joint Chiefs of Staff, Combating Weapons of Mass Destruction, I-40.
- Chappell, Bill. 'Petya' Ransomware Hits at Least 65 Countries; Microsoft Trace it to Tax Software. NPR. (2018), pp. 5-8.
- Chen, Cyberterrorism after Stutxnet, p. 4.
- Choi, S. W. (2010). Fighting terrorism through the rule of law? *Journal of Conflict Resolution*, 54 (6), pp. 940-966.
- Chuijka, Adam. The Strategies of Cyber Terrorism, Ottawa, Ontario, (2016), pp. 1-91.
- Cilluffo, Frank J., Sharon L. Cardash, and George C. Salmoiraghi. "A Blueprint for Cyber Deterrence: Building Stability through Strength." *Military and Strategic Affairs*, Vol. 4, No. 3, 2012: pp. 3-23.
- Cohen, L and Felson, M. Social change and crime rate trends: A routine activity approach, *American Sociological Review*, (1997), pp. 588-589.
- Collin Gray, National Security Dilemmas, p. 56.
- Commonwealth Model Law, ITU Model Laws.
- Communication, K. I. (2013). Connected Kenya 2017. Retrieved 11 13, 15, from ICT Authority: <http://www.ict.go.ke/docs/MasterPlan2017.pdf>.
- Communication, K. I. (2013). Connected Kenya 2017. Retrieved 11 13, 15, from ICT Authority: <http://www.ict.go.ke/docs/MasterPlan2017.pdf>.
- Communications Authority of Kenya, Quarterly Sector Statistics Report: Q2 of the Financial Year 2016/2017.
- Communications Authority of Kenya. (2015). First quarter sector statistics report for the financial year 2015/2016. <http://www.ca.go.ke/images/downloads/STATISTICS/Sector%20%20Statistics%20Report%20Q1%202015-16.pdf>.
- Communications Authority of Kenya. (2015). First quarter sector statistics report for the financial year 2015/2016.
- Constitutional implementation in Kenya, 2010-2015: Challenges and prospects, FES Kenya Occasional Paper, No. 5 ISBN: 9966-957-20-0.

- Crosston, M. (2011). World gone cyberMAD: how BMutually Assured Debilitation^ is the best hope for cyber deterrence. *Strategic Studies Quarterly*, 50(1), pp. 100–116.
- Cyber Defense. <https://www.techopedia.com/definition/6705/cyber-defense>.
- David Souter and Monica Kerretts-Makau, “Internet Governance in Kenya – An Assessment for the Internet Society,” *Internet Society*, September 2012, <http://bit.ly/1M0d9xv>.
- Demessie Fantaye, “Horn of Africa Bulletin, November-December 2015” Volume 27 Issue 6
- Denning D. E., ”Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.” <http://www.nautilus.org/info-policy/workshop/papers/denning.html>
- Department of Defense, Annual Report to the President and the Congress
- Erbschloe, Michael. Review of Information Warfare, [www.techsoc.com/warfare.htm](http://www.techsoc.com/warfare.htm).
- Fischer, Eric A. (2005), Creating a National Framework for Cyber security: An Analysis of Issues and Options, February 22, CRS Report for Congress, Order Code RL32777.
- Freedman, L. (2004). Deterrence. Cambridge: Polity Press.
- 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.
- Gady, F.S . Africa Cyber wmd:[http://www. Foreignpolicy.com/articles/2010/03/Africa cyber.wmd](http://www.Foreignpolicy.com/articles/2010/03/Africa-cyber.wmd). (2010), p. 35.
- Gagliardone, I. 2014. “Media Development with Chinese Characteristics.” *Global Media Journal* 4 (2): 1–16. Government of Kenya. 2014. Cybersecurity Strategy. Ministry of Information Communications and Technology.
- Gagliardone, I., & Sambuli, N. (2015). *Cyber Security and Cyber Resilience in East Africa*. Centre for International Governance Innovation.
- Gaycken, Sandro, and Maurizio Martellini. “Cyber as Deterrent.” In *Deterrence and IT Protection for Critical Infrastructures*, edited by Maurizio Martinelli, pp. 1-10. Heidelberg: Springer, 2013.
- Geoffrey S. Corn, Victor Hansen, Richard Jackson, Christopher Jenks, Eric Talbot Jensen and James A. Schoettler, *The law of armed conflict: An operational approach*. Volume 94 Number 886, 2012
- Gercke, M. The Slow Wake of a Global Approach Against Cybercrime, *Computer Law Review International*, (2006), p. 89.
- Gesser, U., Maclay, C., AND Palfrey, J. (2010). Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations, an Exploratory Study by Barkman Center for Internet and Society at Harvard University in collaboration with UNICEF. [Http//www.cyber digital safety.developing.nations](http://www.cyberdigital.safety.developing.nations).
- Global Cybersecurity Index (GCI) 2017.
- Government of Kenya. 2014. Cybersecurity Strategy. Ministry of Information Communications and Technology.
- Gray, National Security Dilemmas, 2011, 59.

- Itnewsafrika.com.(2011).Smartphone's Will Drive Africa's Internet Uptake.<http://www.itnewsafrika.com/2011/08/smartphones-will-drive-africa>.
- ITU, Global Cybersecurity Index (GCI) 2017
- ITU. 2015. ICT Statistics. [www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx](http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx).
- Ivita Kĩsnica, Organization and individual security: Collective Monograph, [https://www.theseus.fi/bitstream/handle/10024/153249/Organisation\\_and\\_Individual\\_Security.pdf?isAllowed=y&sequence=1](https://www.theseus.fi/bitstream/handle/10024/153249/Organisation_and_Individual_Security.pdf?isAllowed=y&sequence=1); <https://ruor.uottawa.ca/>
- J. Boone Bartholomees--National Security Policy and Strategy
- Jehle, G. A., & Reny, P. J. (2001). *Advanced microeconomic theory* (2nd Ed.). Boston: Addison-Wesley Longman.
- John J. Klein, *Deterring and Dissuading Cyberterrorism*, *ASPJ Africa & Francophonie*, 2018 ; Gray, *National Security Dilemmas*, 2011, p. 72.
- John, O.S. Growth and other good things, *The Economist*, (2013), p. 108.
- Judith M. C. Tembo, "Workshop on Tanzania National Transposition of SADC Model Law", 4th–5th February, 2013,.
- Juma V. (2010) Online Shopping Kenya Consumers Out of KRA Reach. [Http://www.businessdailyafrica.com](http://www.businessdailyafrica.com).
- Kaldor, M. (2003). *Global Civil Society: Answer to War*. Polity Press, Cambridge. pp. 149-158
- Kamau, M (2011), Policy Site Defacing Shows Cyber Crime is Rising.
- Kemibaro, M. (2011, October). Safaricom CLOUD: Safaricom's third act to dominate Kenya's telecoms sector? <http://www.moseskemibaro.com/2011/10/29/safaricomcloud-safaricom-thirdact-to-dominate-kenyas-telecoms-sector/>.
- Kenya Community Support Centre., *Kecosce Annual Report - 2013 - (KECOSCE, 2013)*. Retrieved 23 December 2018, from [http://www.kecosce.org/downloads/kecosce\\_organizational\\_annual\\_report\\_2013.pdf](http://www.kecosce.org/downloads/kecosce_organizational_annual_report_2013.pdf)
- Kenya Cyber Security Report, (2016), p. 14.
- Kenya Gazette Supplement No. 60 (Acts No. 5). *The Computer Misuse and Cybercrimes Act, 2018*
- Kenya Information and Communications (Amendment) Act, (2013).
- Kigen, et al, 2014. "Kenya Cybersecurity Report 2014." [www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf](http://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf).
- Kinyanjui, K. (2009b). Watchdog Warns of Increasing Cybercrime Threat. [Http://www.Businessdailyafrica.com](http://www.Businessdailyafrica.com)
- Knopf, Jeffrey W. "The Fourth Wave in Deterrence Research." *Contemporary Security Policy*, Vol. 31, No. 1 April 2010: pp. 1-33
- Kothari, C.R. *Research Methodology-Methods and Techniques*, New Age International Publishers, (2011), p. 11.
- Kydd and Walter, "The Strategies of Terrorism," 2006, pp. 64-65.
- Leavitt, H. J. (1951). Some effects of certain communication patterns on group performance. *Journal of Abnormal and Social Psychology*, pp. 46, 38-50.

- Lee, Robert. Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center, (2016), pp. 7-13.
- Leedy, Paul. Practical Research. New Jersey: Prentice-Hall, (1997), p. 1.
- 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.
- 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.
- Long, Deterrence, 17–22, 59–61, explains this phenomenon at length, as does Libicki, Cyberdeterrence and Cyberwarfare, 32–35.
- Lye, K. W. and Wing, J. M. (2005). Game strategies in network security. International Journal of Information Security, 5(1), pp. 1–10.
- Maina (2010), A survey on impact of ICT on Business Value Creation in Kenya Banking Sector. Unpublished MBA project, University of Nairobi.
- Maliti T. (2010). New Cables to Tie Africa to Internet, <http://www.washingtontimes.com/news/2010/sep/1/new-cables-to-africa-to-internet>.
- Mark Widdowson, British Association for Counselling and Psychotherapy, <https://onlinelibrary.wiley.com/doi/pdf/10.1080/14733145.2012.697473>
- Marshall Center., PTSS 16-12 Participants Study Civil Society's Role in Defeating Terrorism, Counter Terror Financing. (2016). Retrieved 23 December 2018, from <http://www.marshallcenter.org/MCPUBLICWEB/de/nav-main-more-employmentde/62-cat-english-en/cat-gcmc-pao-en/cat-gcmc-pao-news-en/2028-ar-news-2-25-jul-16-en.html>
- Matusitz and Minei, "Cyberterrorism: Its Effects on Health-Related Infrastructures," 2009, p. 168.
- Matusitz, Jonathan(2009) 'A Postmodern Theory of Cyberterrorism: Game Theory', Information Security Journal: A Global Perspective, 18: pp. 6, 273 — 281
- Mayssa Zerzri, The Threat of Cyber Terrorism and Recommendations for Countermeasures, (2017)
- McKenna, K. Y. A., & Bargh, J. A. 1998. Coming out in the age of the internet: identity Bdemarginalization^ through virtual group participation. Journal of Personality and Social Psychology, 75(3), pp.681–694
- Mugenda, Abel and Mugenda, Olive. Research methods dictionary. Nairobi, Kenya arts press, (2012), pp. 12-13.
- Mugenda, O.M., & Mugenda, A.G. (2010). Research methods qualitative & quantitative approaches. Nairobi: African Centre for Technology Studies
- Muhumuza, M (2010), East Africa EAC Prone to Cyber Crime, say experts. <Http://www.allafrica.com/stories/201008240531>.
- Mwenesi, S. 2014a. "ICT Contribution to Kenya's GDP now at 12.1%." Human IPO, July 22. [www.humanipo.com/news/46203/ict-contribution-to-kenyas-gdpnow-at-12-1](http://www.humanipo.com/news/46203/ict-contribution-to-kenyas-gdpnow-at-12-1).
- NATO Cyber Cooperative Cyber Defence Center of Excellence Tallin Estonia. <https://ccdcoe.org/cyber-definitions.html>.

- Neal, S., Business as Usual? Leveraging the Private Sector to Combat Terrorism. Perspectives On Terrorism, 2(3). (2010). Retrieved 23 December 2018 from <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/31/html>
- Nidhi Prabhu, Social Engineering: The Elusive Adversary in Cybersecurity, September, 2018 Norton Cyber-Crime Report, (2016), p. 79.
- Oliphant, Roland and McGoogan, Cara. NATO warns cyber attacks 'could trigger article 5' as world reels from Ukraine hack. The Telegraph. (2017), pp. 91-21.
- Otuki, N. 2014. "Beijing Says Runda Fraud Ring Likely Targeted China." Business Daily, December 5. [www.businessdailyafrica.com/Beijing-says-Runda-fraud-ring-targeted-China/-/539546/2546306/-/item/0/-/v9hr5bz/-/index.html](http://www.businessdailyafrica.com/Beijing-says-Runda-fraud-ring-targeted-China/-/539546/2546306/-/item/0/-/v9hr5bz/-/index.html).
- Paul K. Davis and Brian Michael Jenkins, Deterrence & Influence in Counter-terrorism: A Component in the War on al-Qaeda (Santa Monica: RAND, 2002), [http://www.rand.org/pubs/monograph\\_reports/MR1619/MR1619.pdf](http://www.rand.org/pubs/monograph_reports/MR1619/MR1619.pdf).
- Paula, K., Carol, M., Kevin, K., Martin, M., & Barbara, S. (2014). Kenya Cyber Security Report 2014. Nairobi.
- Peeter Lorents, Rain Ottis, and Raul Rikk, "Cyber Society and Cooperative Cyber Defence," a paper presented at the 3rd International Conference on Internationalization, Design, and Global Development, San Diego, CA (2009), p. 184,
- Possony, S. T. (1946). Atomic power and world order. The Review of Politics, 8(4), pp. 533–535.
- Powell, R. (2008). Nuclear deterrence theory: the search for credibility, Digitally printed version. Paperback Re-Issue. Cambridge: Cambridge University Press.
- Ranz-Stefan, G. Foreign policy: Africa's internet threat, National Public Radio, (2010), p. 29.
- Regional Conference On Countering Violent Extremism, "Outcome Document - Deepening Cooperation in Countering Violent Extremism," Kenyatta International Conference Centre, Nairobi, Kenya, 25 to 28 June 2015
- Sallhammar, K., Helvik, B. E., and Knapskog, S. J. (2005). Incorporating attacker behavior in stochastic models of security. In Proceedings of the 2005 International Conference on Security and Management, Las Vegas, NV.
- Schelling, Thomas C., and Harvard University Center for International Affairs. 1966. Arms and influence. Yale University Press.
- Schelling, Thomas, The Strategy of Conflict (Cambridge, MA: Harvard University Press, 1960), p. 9.
- Section 3, Draft Cybercrime Bill of Kenya (2014).
- 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>.
- Shane Harris, "The Cyberwar Plan: It's Not Just a Defense Game; Cyber-Security Includes Attack Plans Too, and the U.S. Has Already Used Some of Them Successfully," National Journal, 14 November 2009, [http://www.nationaljournal.com/njmagazine/cs\\_20091114\\_3145.php](http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php).

- Siang-tse, Foo and Jayakumar, Shashi. *Cyber Threats: 2018 and Beyond*, Rajaratnam School of International Studies, NTU. (2018), pp. 2-3.
- SPSS Tutorials, [www.spss-tutorials.com/spss-what-is-it/](http://www.spss-tutorials.com/spss-what-is-it/).
- Stuart Macdonald, Lee Jarvis, Tom Chen, and Simon Lavis, *Cyberterrorism: A Survey of Researchers*, Cyberterrorism Project Research Report No. 1 (Swansea University, 2013). Available at <http://www.cyberterrorism-project.org> (accessed 28 October, 2018).
- Symantec Corporation, (2012), p. 107.
- Symantec Corporation, *Internet Security Threat Report 2013, 2012 Trends, Volume 18*. Available from [www.symantec.com/content/en/us/enterprise/other\\_resources/bistr\\_main\\_report\\_v18\\_2012\\_21291018.en-us.pdf](http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v18_2012_21291018.en-us.pdf).
- Symantec Corporation. *Internet Security Threat Report 2018, the 2018 Trends, Volume 13* (2018), p. 24.
- The Christian Science Monitor., *New encryption technology is aiding terrorists, intelligence director says*.
- The East African, *Kenya Launches Centre to fight cybercrime*, (2016).
- The *Nendo report*. 201411 highlighted the rise and growing power of Social Media influencers.
- U.S. Department of State “Counter Threat Finance and Sanctions,” [State.gov](http://State.gov), available
- U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1–02 (Washington, DC: November 8, 2010), 214, available at: [http://ra.defense.gov/Portals/56/Documents/rtm/jp1\\_02.pdf](http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf).
- UNODC *Comprehensive Study on Cybercrime*, 2013.
- UNODC, *World Drug Report 2013* (United Nations publication, Sales No. E.13.XI.6).
- Wechuli A. (2014) on *Cyber Security Assessment Framework: Case of government Ministries in Kenya*; *International Journal of Technology in Computer Science and Engineering*, 1(3).
- Wilson, “*Cyber Threats to Critical Information Infrastructure*,” 2014, p. 131.
- Zagare, F. C., & Marc Kilgour, D. (2000). *Perfect deterrence*. Cambridge Studies in International Relations

### **Internet Sources:**

- <http://docplayer.net/33090211-Errors-in-sample-surveys.html>
- <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf>
- <http://lc.org/PDFs/StateDeptReportonTerrosirsm2016COMPRESSED.pdf>
- [http://usiofindia.org/article\\_july\\_sep06\\_9.htm](http://usiofindia.org/article_july_sep06_9.htm)
- <http://www.nation.co.ke/counties/mandera/Shabaab-attack-again-Mandera/1183298-3484586-format-xhtml-144hmmu/index.html>



<http://www.secure.nsw.gov.au>  
<https://ca.go.ke/industry/cyber-security/overview/>  
<https://ccdcoe.org/>  
<https://en.wikipedia.org/wiki/Cyberterrorism>  
<https://gomedici.com/social-engineering-elusive-adversary-cybersecurity/>  
<https://nairobi.news.nation.co.ke/news/safaricom-lost-sh20-million-to-fraudsters-this-year>  
[https://suissebank.com/sites/default/files/SB\\_Application\\_Form\\_SBLC\\_EN.pdf](https://suissebank.com/sites/default/files/SB_Application_Form_SBLC_EN.pdf)  
<https://techweez.com/2018/12/09/mpesa-service-outage/>  
<https://www.businessdailyafrica.com/news/M-Shwari-downtime-persists-for-fifth-day/539546-4244684-1mdt8m/index.html>  
<https://www.chrips.or.ke/publications/policy-brief/a-policy-content-evaluation-of-kenyas-national-strategy-to-counter-violent-extremism/>  
[https://www.giac.com/practical/GSEC/Shamsuddin\\_Abdul\\_Jalil\\_GSEC.pdf](https://www.giac.com/practical/GSEC/Shamsuddin_Abdul_Jalil_GSEC.pdf)  
<https://www.ijmsh.com/articles/eBOOK%20for%202015FINALII.pdf>  
<https://www.ncsc.gov.uk/topics/patch-management>  
Imran Awan, Cyber-Extremism: Isis and the Power of Social Media. April 2017, Volume 54, Issue 2, pp 138–149. <https://doi.org/10.1007/s12115-017-0114-0>

## **Appendices**

### **Appendix I: Letter of Introduction**

Date ...../...../2018

TO WHOM IT MAY CONCERN

Dear Sir/Madam:

#### **REQUEST FOR COLLECTION OF DATA**

My name is **Mark M. Ogonji**, a Masters student at the Institute of Diplomacy and International Studies, College of Humanities and Social Sciences, University of Nairobi.

I am conducting a research study titled “**PROMOTING SECURITY IN AFRICA THROUGH EFFECTIVE COUNTER CYBER TERRORISM STRATEGIES: A CASE STUDY OF KENYA**”.

You've been chosen to become part of this study. Help fill in the enclosed interview guide.

The information provided will be treated strictly confidential and will be used exclusively for academic purposes.

Your support and cooperation will be highly appreciated.

Yours Sincerely,

**Mark M. Ogonji**

## Appendix II: Data Collection Instrument

Serial No.....

My name is Mark Ogonji a Masters student in the University of Nairobi's Institute of Diplomacy and International Studies currently undertaking my research project. The main aim of this project is to examine how security can be promoted in Africa through effective counter cyber *terrorism* strategies using the case study of Kenya. The research work requires that I collect field data.

You have been identified as one of the sample of my study. I would be grateful if you could give me your time to respond to these questions. Your response shall be used solely for the purpose of this academic research and shall be treated with utmost confidentiality. Thank you for your cooperation.

Sign.....

Date.....

## Appendix III: Questionnaire

### Instructions

The questionnaire is for academic purposes only and intends to promote security in Africa through effective counter cyber terrorism strategies: a case study of Kenya. Please answer the questionnaire by writing a short statement or marking the appropriate boxes.

### Section 1: Demographics

1. Gender?            Male                       Female
2. Age?  below 30 years    30-39 years    40-49years    50-59 years    60+ years
3. Occupation specialization?.....
4. Name of Organisation?.....
5. How long have you worked for this organization?.....
6. Education level? Secondary   Tertiary College   Undergraduate   Postgraduate  
Other (specify)

### Section 2: Nature and Status of Strategies and Infrastructure to fight Cyber Terrorism

1. a). Have you heard of cybercrime?

Yes                      No

- b). List types of cyber crimes in Africa

.....  
.....

2. List and briefly explain any 5 cyberterrorism incidents you know

.....  
.....

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

Have you experienced any form of cyber terrorism?

- Yes             No

.If yes, explain what happened

.....  
.....

**3.** What are the underlying causes of cyber terrorism today?

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

**4.** The following are various elements of cyber terrorism. Rank the elements in order of their importance.

<b>1.</b>	State sponsored	
<b>2.</b>	Cyberspace surveillance and monitoring	
<b>3.</b>	Political/ideological motive	
<b>4.</b>	Criminal or illegal	
<b>5.</b>	Random or indiscriminate attack	
<b>6.</b>	Non-state actors	
<b>7.</b>	Violence against people or property	
<b>8.</b>	Civilian targets	

9.	Digital means or targets	
10.	use of cyberspace	
11.	Attack on critical infrastructure	
12.	Convergence of real and virtual worlds	
13.	Attack on essential services	

In your opinion, are there important elements missing from the list? If yes, which ones?

.....

.....

.....

### Section 3: Strategies to Fight Cyber Terrorism in Kenya

1. To what extent have the following entities been involved in the fight against cyber terrorism?

	Very Low Extent	Low Extent	Average Extent	High Extent	Very High Extent
National Police Service	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
National Counter Terrorism Centre	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
National Intelligence Service	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Directorate of Criminal Investigation	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Kenya Defence Forces	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Communication Authority of Kenya	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

Private Sector	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Media	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Religious Sector	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
NGOs	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
International Organizations	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

Explain:.....  
.....  
.....  
.....

2. To what extent could the following measures contribute to curbing cyber terrorism?

	<b>Very Low Extent</b>	<b>Low Extent</b>	<b>Average Extent</b>	<b>High Extent</b>	<b>Very High Extent</b>
National Cyber Security Framework	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Cyber deterrence	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Cyber defence	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Cyber dissuasion	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Legislation	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Capacity building and awareness	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Application of Technology	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Regional/international cooperation	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Multi-agency approach	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

Institutional capacity	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Data protection regulations	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Establishment of CSIRTs	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

3. To what extent do you consider that the overall efforts deployed so far in confronting cyber terrorism in Kenya are effective?

<b>Very Low Extent</b>	<b>Low Extent</b>	<b>Average Extent</b>	<b>High Extent</b>	<b>Very High Extent</b>
<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

Explain:.....  
.....  
.....

4. Do the strategies employed by GoK involve:

a) Civil Society?  YES  NO

Explain:  
.....  
.....  
.....  
.....

b) Local Communities?  YES  NO

Explain:  
.....  
.....  
.....  
.....



c)Private Sector?  YES  NO

Explain:

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

d)Multi-Agencies?  YES  NO

Explain:

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

e)International partners?  YES  NO

Explain:

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

**5. What should be the main priorities in order to effectively counter cyber terrorism?**

Please select 4 in the list below and rank them.

1.	Addressing economic and social root causes (unemployment, inequalities)	
2.	Better intelligence sharing between African countries	
3.	. Combating the spread of hate speech, promotion of violence and dissemination of terrorist propaganda online	
4.	Engaging communities: local initiatives can generate a climate of trust and enhance cooperation on the ground	
5.	Facilitating information circulation between security/intelligence services and local authorities/religious communities	

6.	Cyberspace surveillance and monitoring	
7.	Initiating de-radicalization measures	
8.	Promoting good governance, democracy and human rights	
9.	Military response to cyber attacks	

Any other option

.....  
 .....

**Section 4: Effects of Cyber Terrorism on National Security**

1. To what extent do you consider that the following phenomenon threaten the security and stability of Kenya?

	<b>Very Low Extent</b>	<b>Low Extent</b>	<b>Average Extent</b>	<b>High Extent</b>	<b>Very High Extent</b>
Cyber attacks	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Online radicalization	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Hacking	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Website defacement	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Denial of Service	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

.....  
 .....

2. What are the effects of cyber terrorism on the following?

	<b>Very Low Extent</b>	<b>Low Extent</b>	<b>Average Extent</b>	<b>High Extent</b>	<b>Very High Extent</b>
Economic security	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Human Security	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Military	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
Politics	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

Explain.....  
.....  
.....

3. What are some of the preparations the country has made for an imminent cyber terror attack? Please rank them.

1.	Establishment of Computer Security Incident Response Team (CSIRT)	
2.	Establishment of multi-agency counter terrorism strategy	
3.	Legislation of Computer Misuse and Cybercrime Act 2018	
4.	Establishment of Cyber Command Centres	

Explain:  
.....  
.....  
.....

4. What are some of the manifestations of cyber terrorism in Kenya today?

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

5. a) In your view, does cyber terrorism constitute a threat?


Yes

No

b) If so, against whom or what is the threat focused?

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

## Appendix IV: NACOSTI Research Authorisation



**NATIONAL COMMISSION FOR SCIENCE,  
TECHNOLOGY AND INNOVATION**

Telephone: +254-20-2213471,  
2241349, 3310571, 2219420  
Fax: +254-20-318245, 318249  
Email: dg@nacosti.go.ke  
Website : www.nacosti.go.ke  
When replying please quote

NACOSTI, Upper Kabete  
Off Waiyaki Way  
P.O. Box 30623-00100  
NAIROBI-KENYA

Ref. No. **NACOSTI/P/19/12766/27752** Date: **17<sup>th</sup> January, 2019**

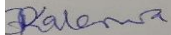
Mark Mbock Ogonji  
National Defence College  
P.O. Box 24381-00502  
**NAIROBI.**

**RE: RESEARCH AUTHORIZATION**

Following your application for authority to carry out research on *“Promoting security in Africa through effective counter cyber terrorism strategies: A case study of Kenya”* I am pleased to inform you that you have been authorized to undertake research in **all Counties** for the period ending **17<sup>th</sup> January, 2020.**

You are advised to report to **the County Commissioners and the County Directors of Education, all Counties** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit **a copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

  
**ODFREY P. KALERWA MSc., MBA, MKIM**  
**OR: DIRECTOR-GENERAL/CEO**

Copy to:

the County Commissioners  
all Counties.

the County Directors of Education  
all Counties.

National Commission for Science, Technology and Innovation (NACOSTI) 2019

## Appendix V: NACOSTI Permit

THIS IS TO CERTIFY THAT:  
**MR. MARK MBOCK OGONJI**  
**of NATIONAL DEFENCE COLLEGE,**  
**24581-S02 NAIROBI,** has been permitted  
to conduct research in **All Counties**


on the topic: **PROMOTING SECURITY IN  
AFRICA THROUGH EFFECTIVE COUNTER  
CYBER TERRORISM STRATEGIES: A CASE  
STUDY OF KENYA**

for the period ending:  
**17th January, 2020**

*Mark Mbock Ogonji*  
Applicant's  
Signature

*Graciano*  
Director General  
National Commission for Science,  
Technology & Innovation

Permit No : **NACOSTI/P/19/12766/27752**  
Date Of Issue : **17th January, 2019**  
Fee Received : **Ksh 1000**




**THE SCIENCE, TECHNOLOGY AND  
INNOVATION ACT, 2013**


The Grant of Research Licenses is guided by the Science,  
Technology and Innovation (Research Licensing) Regulations, 2014.

**CONDITIONS**

1. The License is valid for the proposed research, location and specified period.
2. The License and any rights thereunder are non-transferable.
3. The Licensee shall inform the County Governor before commencement of the research.
4. Excavation, filming and collection of specimens are subject to further necessary clearances from relevant Government Agencies.
5. The Licensee does not give authority to transfer research materials.
6. NACOSTI may monitor and evaluate the licensed research project.
7. The Licensee shall submit one hard copy and upload a soft copy of their final report within one year of completion of the research.
8. NACOSTI reserves the right to modify the conditions of the License including cancellation without prior notice.

National Commission for Science, Technology and Innovation  
P.O. Box 30623 - 00100, Nairobi, Kenya  
TEL: 020 409 7060, 0713 788787, 0735 404245  
Email: [ds@nacosti.go.ke](mailto:ds@nacosti.go.ke), [registry@nacosti.go.ke](mailto:registry@nacosti.go.ke)  
Website: [www.nacosti.go.ke](http://www.nacosti.go.ke)

  
**REPUBLIC OF KENYA**

  
**National Commission for Science,  
Technology and Innovation**

**RESEARCH LICENSE**

Serial No.A 22774  
**CONDITIONS: see back page**

I am pleased to inform you that you have been authorized to undertake research in all