UNIVERSITY OF NAIROBI

INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES

EMERGING CYBER SECURITY THREATS: A COMPARATIVE STUDY OF KENYA AND ZIMBABWE

FARAI TARUVINGA

REG NO: R50/ 35350/2019

SUPERVISOR: DR. PATRICK MALUKI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT FOR REQUIREMENT OF A MASTERS DEGREE IN INTERNATIONAL STUDIES AT THE INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES (IDIS), UNIVERSITY OF NAIROBI

2020

DECLARATION

This Research Project is my original work and has not been presented for a degree in any other University.

Farai Taruvinga……Date……

This Research Project has been submitted for examination with my approval as University Supervisor.

Dr Patrick Maluki……..Date……

DEDICATION

This work is dedicated to my family who believed in me and has always supported me in their own special way. Thank you and God bless you!

ACKNOWLEDGEMENT

I highly appreciate the contribution and support received from various individuals for the successful completion of this research Project. I wish to express my sincere appreciation to my supervisor Dr. Patrick Maluki for his academic guidance and the value he added to my study. I acknowledge the encouragement and inspiration of my family and friends who supported me in their own special way.

ABSTRACT

This research study aims at assessing the emerging cyber security threats: utilising a comparative study of Kenya and Zimbabwe. Emergence and growth of cyber security threats has become a global problem affecting both human and national security of developed and developing states worldwide. However, majority of states in the African region do not have the mechanisms in place to defend or fight the emerging cyber security threats. The lack of such mechanisms in place reduces the main function of any state to provide security and welfare to its citizens. Therefore, there is need for robust cyber threats defence mechanisms, so as to withstand the anticipated cyber-attacks. The general objective is to investigate the cyber security defense mechanisms in place in both Kenya and Zimbabwe in response to the emerging cyber security threats. It was guided by the following specific objectives which include; to examine the legal frameworks put in place in Kenya and Zimbabwe to respond to Cyber security threats, to assess the cyber defences available in Kenya and Zimbabwe to counter cyber security threats and to establish the regional cyber security defence strategies incorporated by the two countries in combating cyber security crimes or threats.in order to conceptualise the study it utilised the Securitisation theory. Their viewpoint centres on the fact that states always struggle to maintain their security. Their referent object is the observed area of the state that is under threat and hence needs to be protected for the state to survive. This research gathered data from both secondary and primary sources. Questionnaires and interview guide were administered to obtain primary data from a sample size of 70 participants from both countries while literature review from varied sources was incorporated to procedure knowledge concerning this research. Both qualitative and quantitative data was analysed through content analysis. The study established that, whereas, Kenya has enacted a number of cyber security related legislations, Zimbabwe on the other hand lacks a comprehensive "Cyber security framework" anchored in law, which could inform national strategy on cyber security. However, respective government key security stakeholders have made efforts to curb the menace especially in the ICT sector. It's also notable that, a number of regional and continental-wide legislative frameworks have been adopted by the two countries and domesticated into national laws. Various recommendations from the study can be made which include: good cyber security policies and practices should put people and their rights, at the centre and seek to strengthen and protect human rights rather than curtail them. More so, cyber security frameworks must include data protection laws which safeguard against the exploitation of personal data collected by companies and public bodies.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

ACNSI- African Cyber National Security Institute

APEC- Asia-Pacific Economic Cooperation

AU- Africa Union

AUCSC- African Union's Cyber Security Convention

BAZ- Broadcasting Authority of Zimbabwe

BCCCR- Budapest Convention on Cyber Crime Resolutions

CAK-Communication Authority of Kenya

CCSP- Convention on Cyberspace Security and Protection

EASSy- The Eastern Africa Submarine Cable System

ECOWAS- West African Economic Community nations

FIRST- Forum of Incident Response and Security Teams

GDT- General Deterrence Theory

HIPSSA-Harmonisation of Information and Communications Technology Policies in Sub-Saharan Africa

IBM- International Business Machines

ICJ- The International Court of Justice

ICT-Information and Communications Technology

IL-International Law

ITU- International Telecommunications Unit

KDF- Kenya Defence Forces

KIC- Kenya Information and Communication

KNISA-Kenya National Intelligence Service Act

MIC- Media and Information Commission

MICNG- Ministry of Interior and Coordination of National Government

NCS- National Communication Secretariat

NCSC- National Cyber Security Committee

NCSMP-National Cyber Security Master Plan

NCSMS- National Cyber Security Master-plan and Strategy

NPS- National Police Service

OECD- Organisation for Economic Co-operation and Development

PCK- Postal Corporation of Kenya,

POTRAZ- Postal and Telecommunications Regulatory Authority of Zimbabwe

PXR- Protocol of Xenophobia and Racism

SADC- South African Development Cooperation

SCOISA- Shanghai Cooperation Organisation's Information Security Agreement

STA- Science and Technology Act

T-AJCCC- Trans-Atlantic Joint Cyber Cell Collaboration

TCK-Tel Company Kenya

TK- Telkom Kenya

UN- United Nations

UNDHR- The Universal Declaration of Human Rights

UN-GCSE- Group of Cyber Security Experts

USA-CTIIC Cyber Threat Intelligence Integration Center

WACS- The West Africa Cable System

SEACOM- SEACOM (African cable system)

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1.0 Introduction

Cyber security threat is a phenomenal threat brought about by developments in ICT. The ITU explains cyber security as the efforts aimed at safeguarding the cyberspace environment and its users from all threats that might threaten their security as well as that of the nation.[1] Threat is an occurrence instigated by volatile natural or premeditated actions having undesirable consequence, upon an organisation or state inducing deviations in normal functions.[2] As a result, from the above definitions, cyber security threats then combine all electronics related gadgets and threats posed to the national security of states.

There are trends in the national security of different states globally. States are implementing strategies for cyber security defence arising from cyber security threats which are domicile in cyber space. However, a state that disregards the importance of protecting its space is doing so to her peril. This particular state is guaranteed of insecurities in the volatile, uncertain, complex and ambiguous environment as she pursues her national interests.[3] The cyber security threats effects are now affecting states which are still having less established and developed agencies, for cyber defense in their institutions of national power. Therefore, there is need for robust cyber threats defense mechanisms, so as to withstand the anticipated cyber-attacks.

1.1 The Background of the Study

Cyber security came about as a result of developments in ICT. The cyber

[1] Kabanda,G. (2020). *A Cyber security Culture Framework and Its Impact on Zimbabwean Organizations*. Honolulu, Hawaii: Atlantic International University

[2] Buzan, B., & Little, R. (2000). *International Systems in World History: remaking the study of International Relations.* New York: Oxford University Press

[3] Amos, A. (2009). *American Security*, 6th Ed., Baltimore: The Johns Hopkins University Press

security threats became pronounced in Africa from 2007 through reading the attacks from Eastern Europe. The first cyber-attack took place in Estonia in 2007 and was conducted through use of networked computers.[4] African states started to use computerised systems both in administration and business transactions in 2007 as well.[5] However, the attack led to the birth of cyber warfare. The networked computers provided a good platform for cyber warfare to be conducted. Worth noting is that, cyber war is a war fought with the computer hardware as the guns and software as the ammunition.[6] The virtual ground is the connected and interconnections of computer hardware, through various protocols for their communication.

States throughout the world were disturbed by the Estonia attacks on the national ICT infrastructure. The existence of the state was almost completely destroyed through an online or electronic initiated attack.[7] States began to accept cyber-attacks as a real phenomenon from 2007. For instance, the USA, China and Russia immediately pronounced the cyberspace as their 5th domain of warfare, besides land, air, space and sea.[8] Estonia also began to develop an approach to curb cyber threats in 2007 after the attack which was finally incorporated in the country's national security strategy by 2008.

At this point, the national security arrangements in Estonia provided two observations in the national security strategy implementation, which were in most states throughout the world. Firstly, the governments of most states in Europe had no provisions of the governance mechanisms over the networked telecommunications

[4]Rain, O. (2019). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective Cooperative Cyber Defence Centre of Excellence*. Tallinn, Estonia: Academic Publishing Limited
[5]Ibid, p6.
[6]Ibid, p7.
[7]Ibid, p10.
[8]Baezner, M. (2018). *Cyber- security in Sino-American Relations*. ETH Zurich: Center for Security Studies

and internet infrastructures.[9] Secondly, the cyber security was supposed to be removed from the IT realm, and agencies established that could handle the threats. Third, deliberate political decisions were supposed to be taken in awarding the departments mandated, to defend or fight any existential threats to the states.[10] The state departments with constitutional mandates for national defence or security were supposed to be tasked to develop cyber threats defences.

The failure to deal with threats emerging from the cyber space was compounded by the fact that, in several states there were no proper definitions of functions, institutions, resources and skills. In addition, there were computer technicians and operators, including support engineering departments only. The unknowing disregard of the cyber security component was unintentional. Therefore, for an effective cyber security to function at any level there must be provisions of network, application, identity, data and database, infrastructure, computing power, mobile devices, disaster recovery and business continuity management procedures, as well as end-user education and awareness.

The cyber security resilience can be achieved through the "national cyber security strategy" as was later developed by Estonia. Estonia took a thorough analysis of the cyberspace, dividing it into levels. Every level had its threats and defenses well defined.[11] European region in the realm of its regional collective security as EU further, layered the cyber space to include the mainland Europe and maritime states.[12] In fact, the inclusion of cyber security as a component of the regional collective security plans begun in 2008. In fact, no solitary state or association can uphold active

[9]Rain, O. (2019). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective Cooperative Cyber Defence Centre of Excellence*. Tallinn, Estonia: Academic Publishing Limited

[10]Ibid, p12.

[11]Op Cit

[12]Kelly, J. (2015).Strategic perspectives on cyber-security management and public policies. *European Cyber-security Journal*, 1(1), 26-72

cyber security defence alone without integrating her defenses with various actors and stakeholders in the region.

1.1.1 Security and Securitisation of the Cyber Space

Generally, security is well-defined in terms of perceived survival regarding individuals, states or regions and use of alternative means of combating threats that threatens peace and stability.

On the hand, securitisation is taking of any action that, leads to considerations that the area mentioned would be of security concern.[13] The area of concern can either be defined politically, militarily, intelligently or economically. This implies that, any proclamation by the head of state or government aligns these certain areas, as "the referral objects or subjects of securitisation". The procedure once in existence is portrayed by tightening up all the loose drills of actions necessary to pursue national interests.[14] Therefore, its states mandate to implement the necessary legal, strategies and operational procedures.

Securitisation insinuates that, majority of governments and leaders have made proclamations to the cyber security threats, as a scourge in terms of the obtaining thrusts of enhancing deterrent measures in national and global security. The former President of the USA Barak Obama acknowledged the cyber space and said that, the world has become interconnected by cyberspace and humans cannot escape from it. This merely implies that, the practitioners of the three pillars of the state, executive, legislature and judiciary must ensure that, the area has already been securitised, once the leader of a state has made proclamations of this nature.

---

[13] Buzan, B. (2016). People, States *and Fear: an agenda for international security studies in the post-cold war era.* Colchester: ECPR Press.

[14] Alan, C. *(2003). Security and South East Asia: Domestic, Regional and Global Issues.* Colorado: Lynne Rienne Publishers Inc.

1.2 Statement of the Problem

States in the African region do not have the mechanisms in place to defend or fight the emerging cyber security threats. The legal and institutional frameworks are not yet in place to enhance cyber space defence enforcements. The lack of such mechanisms in place reduces the main function of any state to provide security and welfare to its citizens. This means, states which do not have cyber security mechanisms to defend any perceived threat in the cyber space realm, are short of achieving the national security obligations. The nonexistence of these frameworks and institutions for cyber security defenses are to a large extent, due to the existing national security models that, have maintained the realm of security having the potential of being destabilised or physically invaded especially in the territorial space of a state by another or other states.

Kenya and Zimbabwe have comparable cyber security infrastructure such as the cyber intelligence, cyber defence, cyber protection, cybercrime and human capacity building. Each of these requires certain knowledge, infrastructure, skills, tools, as well as necessary equipment pertinent to the field. Where these functions are neglected including the allocation of responsibilities, they have resulted in separate and uncoordinated activities being carried out unsystematically both at the regional and national levels. Therefore, this study compares the emerging cyber security threats in Kenya and Zimbabwe.

1.3 Research Questions

1. What are the legal frameworks put in place in Kenya and Zimbabwe to respond to cyber security threats?
2. What are the cyber defenses available in Kenya and Zimbabwe to

counter cyber security threats?

3. What are the regional cyber security defence strategies incorporated by the two countries in combating cyber security crimes or threats?

1.3.1 General Objective

To investigate the cyber security defence mechanisms in place in both Kenya and Zimbabwe in response to the emerging cyber security threats.

1.3.2 Specific Objectives

1. To examine the legal frameworks put in place in Kenya and Zimbabwe to respond to Cyber security threats.

2. To assess the cyber defenses available in Kenya and Zimbabwe to counter cyber security threats.

3. To establish the regional cyber security defence strategies incorporated by the two countries in combating cyber security crimes or threats.

1.4 Literature Review

Literature review's purpose is to enable the researcher to acquaint self with the existing studies and topical discussions to the particular area of study, giving details of the available knowledge in the form of a report. The researcher draws attention to the findings and recommendations as assessments of the constraints posed by cyber security threats to national security outlined in other works.[15] The literature review pursues objectives of the study, key terminologies and framework of cyber security threats and national security in Kenya and Zimbabwe.

[15] Kothari, R C, (2003). *Research Methodologies*, 3rd Edition. New Delhi: WishwaPrakashan

1.4.1 Theoretical Literature Review

The theoretical literature review was necessary for this study as it has been used to examine the key debates on cyber security threats. The study considers international relations theory and securitisation theory.

1.4.1.1SecuritisationTheory

Securitisation procedures are the systematic ways of assessing security requirements of the state by prioritising the identified areas of security concerns. The most prioritised area of concern becomes the referral object of the state's national security.[16] According to the proponents of the securitisation theory such as Barry Buzan (1991) from the Copenhagen school, national security involves and incorporates emerging referral objects.[17] Buzan and Little (2000) further propound to the notion by indicating that, the legibility of applying the securitisation theory on any referent object as part of the national security is essential. It also encompasses the study of security issues such as terrorism.[18] In this regard, the two proponents assess the validity of studying independent variables such as terrorism as it affects the dependent variable which is the national security.

Buzan and Little (2000) assert that, the underpinning fact in the national security is that of existential threats through the cyberspace. The threats are pronounced by proponents of national security such as Stephen Walt of the Kennedy School as quoted in by Buzan and Little.[19] The school contents that cyber wars are conducted by the military under the direction and control of states. Statecraft is

[16] David, E. (2005). *The Mosaic Theory, National Security, and the Freedom of Information Act*. *The Yale Law Journal*, 115 (3)
[17]Snow, M. (2004). *National Security for a New Era: Globalization and Geopolitics*. New York: Pearson Education.
[18] Buzan, B & Little, R. (2000). *International Systems in World History: remaking the study of International Relations.* New York: Oxford University Press.
[19]Ibid, p 23.

directly related to military affairs in terms of arms control and crisis management.[20] As such, the state remains influencing the conduct and character of the war.

The Copenhagen school is of the view that, states are not observant of the need to expand the scope of national security studies, to encompass cyber security as this is the only limitation they impose upon themselves.[21] The idea viewed from the cyber security threats is that, the state's physical security and its military capability, are supposed to be integrated in provision of defence for public good of the state's population.[22] It concludes that, states maintained national security as physical security without incorporating the cyber security.[23]

The states are supposed to expand the scope of national security as a result of the emerging cyber security threats. The national security studies and implementation espouse the cyber security threats as the independent variable in the context of national security. A shift in position is realised instead of maintaining the broader view of political, economic, societal and ecological concerns as major components to the national security existence.[24] The rationale is that, security to individual persons as well as states and non-state actors is threatened by cyber security threats, hence needs to be incorporated and coordinated in the national security realm.[25] Cyber security threats need to be regarded as real threats and part of the national security.

Snow (2004) indicates that, the use of the national security is not limited to physical security prescribed issues, but can even be used as an approach to new and

---

[20] Sico van, M. (2018). *State-level responses to massive Policy Brief cyber-attacks: a policy toolbox.* Amsterdam:Clingendael – the Netherlands Institute of International Relations.

[21] Sergei, K., Sergei, K., & Igor, D. (2007). *Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law. Moscow,* Russia: ICTS and international security

[22]Ibid, p 23.

[23]Ibid, p 26.

[24] David, E. (2005). The Mosaic Theory, National Security, and the Freedom of Information Act. *The Yale Law Journal*, 115 (3)

[25]Ibid, p 12.

divergent referent objects of the state for securitisation.[26] He analyses transnational crime as a subject of securitisation as it poses security threats amongst states. Dover ponders on the theory of securitisation and views the emergent issues of immigration as new and divergent threats to security of states and regions.[27] He is of the opinion that, there should be securitisation of the immigration, as the emigrants will form communities in the hosting states that will pose threats to national security, as they demand equality among many other issues.

1.4.1.2 Space Transition Theory

This theory was formulated by K. Jaishankar in the year 2008. The theory views that the cyber space has resulted in emergence of criminal activities and further expound to explain the causing factors of the increased crime rate. It analyses the behavior and character of individual who engage in cybercrimes from one space to another.[28] He posits that, when people move from one place to another they behave differently depending on the environment they encounter with.

In addition the theory proposes factors that led to individuals committing cybercrime which includes; individuals with history of engaging in criminal activities eventually end up engaging in crime in both spaces, persons who indulge in crime will likely transfer it to different areas and lastly, the ideas, norms and characters practised and upheld in physical space may end up conflicting with those of cyberspace, leading to emergency of cybercrime.[29]

He argues that all these factors facilitates to the increased cybercrimes in both

---

[26] Snow, D.M. (2004). *National Security for a New Era: Globalization and Geopolitics*. New York: Pearson Education

[27] Dover, R. (2009). *Towards a Common EU Immigration Policy: a Securitization Too Far.*

[28] Karuppannan, J. (2008). *Cyber criminology & cyber forensics Space Transition Theory of Cyber Crimes.* New Delhi, India: MHRD

[29] Ibid

developing and developed countries which poses a threat to both national and human security. Therefore, there is need for countries to enact stringent measures to curb this menace which is detrimental to the growth and development of the countries.

1.4.1.3 General Theory of Crime and General Strain Theory on Crimes

Cyber space crimes have become a matter of concern in the contemporary modern world. This is due to the increased use of internet, advanced technologies and electronic forms of communication which have transformed the way people interact and eased transfer of information worldwide. This has had both advantages and disadvantages which include cyber bullying as one of the cybercrimes conducted on daily basis mostly through use of internet. These cybercrimes have had serious negative effects on the victims which can eventually lead to suicide or death.

According to general theory of crime as argued by Gottfredson and Hirsch (1990), cybercrimes are carried out by individuals with low self-control who aims at pursuing their own interests in order to maximise pleasure, and they have less or no capacity to control their behavior in safeguarding this pleasure. Presence of available cyber space opportunity combined with low self-control determines whether the individuals will engage in more cybercrimes in their lifetime.[30]

General strain theory argues people engage in crime due to strain. According to Agnew (1992), strain can be broken into three categories which includes; inability to receive a positive valued stimuli, losing the achieved stimuli and fear of emergence of a negative stimuli.[31] As a result they stimulate anger, frustrations, depression and anxiety especially in cases where the strains are perceived as being unfair and can be broken anytime. In efforts to counter this negative emotions and strains, individuals

[30] Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime.* Stanford University Press: Washington D.C.
[31] Ibid

engage in cybercrimes and other criminal activities.

1.5 The Empirical Literature Review

Empirical literature review focused on desktop review from secondary sources related to the area of the study. It was reviewed in line with the study objectives. The objectives sought to assess the legal frameworks available and how they assist in responding to cyber security threats in Kenya and Zimbabwe, cyber defence mechanisms put in place and the regional cyber security defence strategies incorporated by the two countries.

1.6 Legal Frameworks put in place to respond to Cyber security Threats

In the African region, the existence of the cyber-specific laws that govern states is not adequately pronounced.[32] Although this gap in the legal frameworks and provisions of the laws is glaring, this does not mean that there are no rules that govern cyberspace activities.[33] States in regional or sub-regional groupings, agree upon parameters which are the rules that govern the behaviour of the states. The general applicable rules of IL govern behaviour conduct at the cyber space.[34]The IL is applicable to the cyberspace, as a flexible and adequate body of laws, with power to regulate the regions and states, once they are institutionalised.

The structure of the IL itself makes it adaptive and accommodative to the advent of new phenomenon, such as the cyberspace security and the inherent

[32]Stefan, F. (2005).*Cyberspace Security: A definition and a description of remaining problems*. Vienna: University Vienna - Institute of Government & European Studies
[33]James, L., & Katrina, T. (2011). *Cyber-security and Cyber-warfare, Preliminary Assessment of National Doctrine and Organization.* Washington, D.C.: Center for Strategic and International Studies
[34]Dighton, F. (2015). , *Defining a Framework for Decision Making in Cyberspace: Strengthening Cyber-security Series.* Pennsylvania: Indiana University Press

operations, hence there is need for efforts to regulate these operations.[35] The operations in the cyber space and methodologies, tools and instruments applied in the processes, qualify to be governed by IL, as it was used to govern the nuclear weapons.[36]

1.6.1 International Court of Justice Capacity to Handle Cyber Security Issues

The ICJ used the same instruments of the IL and succeeded in interpreting the law to deal with the dilemma of the nuclear weapons. The ICJ addressed the concerns of these weapons after the IL had been in force.[37] The actual aspects of the IL that address the cyberspace operations are those provisions, that are binding on the use of force, without considering the weapon used.[38] It is true that, the particular cyber weapons are now in existence and a particular domain of warfare has been pronounced. Applying the same principle of the IL, cyber operations are governed by the same instruments of IL, that govern nuclear weapons with no ambiguity. Therefore, it can be concluded that, IL is adequate to address cyber space security dilemma. In this regard, it is attainable for states to cooperate and integrate their efforts in the cyber space operations, by creating synergies in combating the cyber security threats.

1.6.2 United Nations response on Cyberspace Operations

UN as a supranational body deliberated and made efforts to normalise the cyber space operations. The main arguments that were presented included those of the

[35]Lars, B., Steffen, J., & Finn, S. (2007). *The Security-Development Nexus Expressions of Sovereignty and Securitization in Southern Africa*. Cape Town, South Africa
[36]CyberCity,E. (2018).*Media Statement SADC Capacity Building Workshop on Cyber Security and SADC Regional Cyber Drill.* Mauritius
[37]Ibid, p 34.
[38]Ibid, p 35.

IL, the applicability of the law and ubiquity in handling the anticipated problems.[39] The other attempt was to bring about open, protected, pacific and manageable cyber milieu.[40] It is also indicated that all sovereign states have laws, principles and norms which guide their behaviour and activities especially in the cyberspace. The UN Charter is clear and asserts that, all states should adhere and respect human rights protocols in their efforts to safeguard the security of cyberspaces.[41] However, according to the UN Charter, it is certain that, states are accountable to the transnational obligations, arising from transnational and illegal actions that are attributed to them.[42] It is inevitably not permissible for states to let or make use of representations to conduct unlawful actions besides safeguarding their cyber spaces.

1.6.3The International Telecommunication Union Purview

The ITU is an Inter-governmental organisation (IGO) created to regulate the functions of the telecommunications bodies of states globally. It also oversees on regional arrangements, agreements, treaties, alliances and sectorial treaties to create frameworks of regulating the cyber space activities.[43] The main contents and governing principles are drawn from the founding ITU Constitution of 1992, the BCCCR in 2001, the PXR in 2006, the SCOISA and the 2014 AUCSC.[44]

The above conventions are limited to regulating the portion of cyber space offences, related to cyber-criminal activities perpetrated through computer systems or meddling with the telecommunications infrastructures. It only enforces behaviour of

[39] Desmond, B., & Gary, W. (2013). Security Challenges. *Journal of Regional Security*, 9(2)
[40], Robert, G. (2012). *International Engagement on Cyber: Establishing Norms and Improving Security*. Washington, D.C., United States: Georgetown University Press
[41]Ibid, p5.
[42]Buzan B. and Waever O, *Regions and Powers: The Structure of International Security*, Cambridge, Cambridge University Press, 2003, p 27-30.
[43] Desmond, B., & Gary, W. (2013). Security Challenges. *Journal of Regional Security*, 9(2)
[44] Lars, B., Steffen, J., & Finn, S. (2007). *The Security-Development Nexus Expressions of Sovereignty and Securitization in Southern Africa*, Cape Town: South Africa

the telecommunications authorities, thus the agencies created in the states to regulate the telecommunications procedures and functions, and not the states themselves.[45] Additionally, states appear disinclined towards involving themselves in the cyber security growth and laws hence, remain stuck in the growth of their municipal laws.

1.6.4 African Union (AU) Cyber Security Strategies

Cyber security threats have been having grave effects on states institutions of power in the African region.[46] It's evident that, eminent growth in cyber space operations threatens the national security of states. These establishments have led to the foundation of the state's existential threat defence mechanisms.[47] The mainstays of the institutes of power are resident in the securitised referral objects of the states, in areas such as the political, military, economic, social-ethno and environment.

The scope of the AU comes with defence mechanism that sought to address wider governmental, commercial or infrastructure networks. This endeavoured to enhance intrusion, prevention and detection, analytic and threat assessment capabilities as well as improve capacities of states to respond to cyber security incidents.[48] Therefore, the AU has made efforts to set regulations in its Charter, which will assist the African states to implement cyber security defenses within their jurisdictions.

1.7 Cyber Security Defense Strategies in the African Region

Studies on some of the adopted models for securitisation and national security posit that, states or non-states actors envisage that, damages to their existence are prevalent, if cyber security defenses implementation were not accomplished. The national

[45]Ibid, p 33.
[46] NirKshetr. (2019). Cybercrime and Cyber security in Africa. *Journal of Global Information Technology* 6-7
[47]Ibid, p 7.
[48]Ibid, p 44.

security is also challenged in the volatile, uncertain, complex and ambiguous environment, where the cyber security has in some cases been left glaringly open. The strategies that govern the cyber space include the integration of the cyber security in the national security.

1.7.1 Integration of the Cyber Security into the National Security

It is prudent to integrate cyber security defence mechanisms into national security defence framework of states, in order to accomplish the national security defence objectives of any states.[49] The implementation of the cyber defence mechanisms indicates that, any scenario which threatens security, whether regionally or nationally can be responded to through the cyber defence mechanism in place. The cyber security defence is an independent variable to the national security defence framework. Therefore, cyber security defenses are emerging phenomenal issues that need to be studied under the national security premises.

With the use of IOT and AI in industry and medical fraternity, the sectors are threatened by the actors in cyber space. Buttressing of the effects is pronounced in the defence and munitions manufacturing industries, where the cyber threat activities are mainly espionages pursued by state or non-state actors to sabotage or steal information. Every state needs to have cyber security defence mechanisms to guard against cyber security threats, by establishing critical agencies even within the existing establishments. The existing threats to most states are the desire to remove the sitting governments through the regime change agenda or breaking away from the state on political lines.[50]

---

[49]Lars, B., Steffen, J., & Finn, S. (2007). *The Security-Development Nexus Expressions of Sovereignty and Securitization in Southern Africa*, Cape Town: South Africa

[50]Cavelty, M. D. (2007). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (1st ed). Boulder: Lynne Rienner

1.8 Cyber Security Response Strategies Frameworks in Africa

The cyber security threats in the Africa region are a concern compared to developed regions such as the Europe and America. The cyber security threats have manifested as a force to reckon within in the regional and nation security. It is further expounded by the fact that, the concepts of safeguarding the cyberspace from possible threats have become an important agenda in most of the African states.[51] The increased awareness is not on an exponential scale, as some other states have remained unassuming in implementation of cyber defence mechanisms, as part of national security agenda. These threats in the continent have fascinated the African region to revise the regional strategic security plans at hand.[52] Africa Union Group of the Experts Report (2019), states that, the region finalised the response strategies and hence needed implementation.

1.9 Research Gaps

Most of the literature available on the cyber security threats legal frameworks and institutions, responses and the relevant strategies in the African region adopted to combat cyber security threats revealed that, there is no or minimal efforts put in place to fight these threats in both countries. The political will to address the cyber security threats as part of the national security is also lacking. The unassertiveness of the securitisation models developed and adopted is not clear in most of the African states. In fact, the general integration of the cyber security into national security strategic plans in most cases is the missing link in the security of the state and security of the cyber space. It is in this vein that, the study seeks to establish the legal frameworks and institutions available defence mechanisms as well as the adopted strategies.

[51]Ibid, p23.
[52]Ibid, p25

1.10 Justification of the Study

The literature review from the available works underlines gaps between cyber security threats and national security synergy. The synergy is not complete as the variables are in the treatises reviewed are inseparable entities. The study looks at the gaps and proffers solutions through undertaking the academic and policy justification of the study.

1.10.1 Academic Justification

There is much research work which has been undertaken on states cyber security threats and national security separately. The non-integrative relationship has not been expounded in the African region.[53] This has resulted in limited efforts in studying the cyber security threats as part of national security. Following the insufficiency in the studies, it is incumbent that, information gaps in regards to the cyber security threats and national security in the African region, is an area that requires further studies.[54] The study intends to generate and contribute more knowledge by assessing these threats, national security policies and strategies in place.

1.10.2 Policy Justification

From the policy related literature, states in developing region such as Africa are affected by inadequate cyber defence, infrastructure, institutions and legal frameworks.[55] States need to establish institutions that will enhance cyber security in the African region. The Asian and East European regions are outstanding as sources of actors in the cyber space, involved in nefarious activities on other states'

[53]Ibid, p 33.
[54]Ibid, p 36.
[55]Op Cit.

infrastructures. This has affected states in the developed regions such as Europe and America.

Despite the lack of institutions, legal frameworks and cyber defenses in the African region, the cyber security is not also integrated into national security.[56] Some states in developed regions such as Western Europe and America are grappling with infringements of the laws in place, although they have integrated the cyber security into their national security.[57] Even though they have initiated harmonisation of the laws, there are disparities that still affect operations of the institutions.

The cyber security defence capability of both Kenya and Zimbabwe presents problems to their national security in the pursuit of the national interests. Therefore, the study will seek to avail knowledge on the policy formulation and implementation as well as modification of the defence capabilities of the two countries in combating the cyber security threats.

1.11 Theoretical Framework

The Securitisation theory was developed by Barry Buzan and Ole Waiver. Their view point centres on the fact that, all states in the anarchic international system always struggle for survival by ensuring their security. Their referent object is the observed area of the state that is under threat and hence needs to be protected for the state to survive.[58] The concerned area of the state presenting a security issue that has existential threat calls for political measures to handle it. In this regard, the referent object or area is then securitised.[59] The process of securitisation follows a procedure

[56]Ibid, p 3.
[57]Ibid, p 19.
[58] Snow, D.M.(2004). *National Security for a New Era: Globalization and Geopolitics*. New York: Pearson Education
[59]Buzan, B., & Little, R.(2000). *International Systems in World History: remaking the study of International Relations.* New York: Oxford University Press

that, before the securitisation, the object is politicised and as the threat continues to escalate, it is securitised. This process begins by a speech act initiated by the political hierarchy of the state with the necessary legitimacy.[60]

The social construction of the security issues can be examined through analysing the legitimate securitising speech acts, as this is the way the prevalence of the threat is made known to the state.[61]The speech work established the point that, there is need for having the prevailing security threat conditions securitised. The felicity conditions of the speech act, leads to the completion of the actions. The securitisation proceeds along an approach which needs acceptance between the state and the organs that address the securitisation. It can be concluded that, securitisation is a political choice as it rests on the conceptualisation of the referent object, in a specific dimension.

The citizenry has to accept the referent object as having an existential threat that is credible hence requires action.[62] The condition is necessary for the speech act to be effective. The speech act must initiate the procedural process of securitisation, which first identifies the existential threat as legitimate for auctioning; through politicisation of the issue in order to bring about measures to combat it effectively. The second point addresses the legitimacy of the securitising authority, in regard to the social and political capability to address the existential threat. The third aspect reviews the historical narrations of the existential threats, the history of the competition rivalry which dictates the pace of securitising the referent object and lastly whether the standard points are enough to securitise a referent object.[63]

[60]Buzan, B. (2016). People, *States and Fear: an agenda for international security studies in the post-cold war era.* Colchester, ECPR Press
[61]Ibid, p72.
[62]Bourne, M.(2004). Understanding Security. London: Palgrave, Macmillan
[63] Buzan, B,. & Waever, O. (2003). *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press.

The inclusion of the sectors in the security realm has brought issues that need to be dealt with in the same manner as they are in sectors preferred. If the sectors are analysed and paying attention to the referent objects in them, it would be clearer that, the evolution in the security realm now encompasses at least everything. This is derived apparently from how states perceive the intentions of one another. This is due to the fact that, the military as a force breaks regular diplomatic relationships by way of disturbing ambassadorial gratitude. In this regard, states national security agenda are geared towards attainment of national security. This is borne from the pertinent assumption made that, in the first instance, the military security is no longer pitched in the realm of the danger of war, but logically have the prevalence of asymmetric effects essentially parallel to war that have to be considered politically.[64]

The political sector regards the peaceful and organisation stability of the state taking aim at the ideology with the principal targets as natural identity, organising ideology and the national institutions. The referent object is the productive principal denoted as independence.[65] Anything that attacks fundamental policies is a serious security issue. Therefore, the cyberspace is used to attack this fundamental principle, through the use of the critical infrastructure, institutions and ideology. As such, there is need to securitise the cyberspace to address the cyber security threats.

1.12 Hypotheses

The study will test the following hypotheses:

a. There are sufficient legal frameworks and institutions in Kenya and Zimbabwe to respond to cyber security threats.

[64]Buzan, B., & Little, R. (2000). *International Systems in World History: remaking the study of International Relations.* New York: Oxford University Press

[65]Snow, D.M. (2004). *National Security for a New Era: Globalization and Geopolitics*. New York: Pearson Education.

b. There are established cyber defenses available in both countries to counter cyber space threats.

c. There are regional cyber defence strategies and mechanisms incorporated by Kenya and Zimbabwe in combating cybercrimes.

.

1.13 Research Methodology

This section provides the research methodology for the study which is sequenced as follows: research design, study site, data collection procedures, target population, sample size determination, validity and reliability of research instruments, sampling procedures, scope of the study, limitation of the study, data analysis as well as ethical considerations.

1.13.1 Study design

The study utilised the descriptive research design which encompasses investigation of population using selected samples to discover and analyse occurrences. It provides a deeper understanding of various dimensions on the cyber security challenges in both Kenya and Zimbabwe. In addition, the study conducted a qualitative research through studying journal articles, related material, academic papers and books on both cyber security threats and national security.[66] To support these efforts, the analytical and descriptive research methods were used to explore the cyber security threats and national security.

1.13.2 Study site

The study was conducted in capital cities of both Kenya and Zimbabwe. Both

[66]Ritchie, J., & Lewis, J. (2004). *Qualitative Research Practice: A Guide for Social Science Students and Researchers.* New Dehli: Sage Publishers

countries have experienced varying cyber space threats which threaten their national security. The researcher sought to conduct interviews with the targeted respondents in Nairobi and also distributed questionnaires. However, in Harare participants were send questionnaires through emails which they answered and returned.

1.13.3 Data Collection Procedures

The study was conducted and complied from the National Defence College, faculty of the University of Nairobi. The interviews were conducted in Nairobi and Harare for the selected interviewees. The researcher conducted the interviews with targeted respondents from Nairobi and Harare, where he got an opportunity to probe them further on the study subject. This ensured validity and authenticity of the data provided. The questionnaires were distributed to the targeted respondents at the NDC faculty.

For the respondents in Zimbabwe, Mrs Manyonga acted as the agent to distribute the questionnaires to different targeted respondents. Once they completed filling/ answering she sent them through DHL to the researcher at the NDC in Kenya. In cases where the participants were not available due to various reasons, the researcher sent them the questionnaires through the emails and engaged others on the phone.

1.13.4 Target Population

The study targeted individual persons, officials in various organisations, ministries and department that partake in the cyberspace operations in both Kenya and Zimbabwe. The researcher targeted persons and officials with relevant knowledge and experience on the study area. The main respondents in Kenya were from the Kenya

ICT Authority, CAK, NIS, Ministry of Defence, NPS and KDF.[67] This included at least five (05) respondents per selected organisation or ministry. Therefore, the researcher targeted 35 respondents from each country drawn from different ministries and departments. Further, since the ministries and departments are not similar in both countries, the 35 respondents drawn from Zimbabwe were from related governments, ministries and departments. The total number was 70 respondents. The lists are shown in Tables 1.1 and 1.2 respectively.

1.13.5 Sample Size/ Sampling Frame

The study utilised a population size of 70 respondents from both Kenya and Zimbabwe. The sample size is composed of key experts and professionals in the subject area. Therefore, it was highly recommended that, if at least 66.7% of the population were utilised for the study in which 23 respondents were drawn from Kenya and Zimbabwe respectively constituting to 46 respondents, the study was deemed fair for analysis.[68]

[67]Creswell, J W. (2014). *Research Design*, 4th Ed. Lincoln: University of Nebraska
[68]Mugenda, A.G. (2011). *Social Science Research, Theory and Principles.*Nairobi: Applied Research & Training Services.

Table 1.1 Population Distribution in Kenya

Serial No.	Organization	Target Population
(a)	**(b)**	**(c)**
1.	Communications Authority of Kenya	5
2.	NDC	5
3.	KDF	5
4.	National Police Service	5
5.	NIS	5
6.	Safaricom	5
7.	Justice	5
	TOTAL	35

Source: Researcher, 2020

Table 1.2 Population Distribution in Zimbabwe

Serial No.	Organization	Target Population
(a)	(b)	(c)
1.	Ministry of ICT and Cyber Security	5
2.	ZNDU	5
3.	ZDF	5
4.	ZRP	5
5.	CIO HQ	5
6.	Ministry of Justice, Legal and Parliamentary Affairs	5
7	Ministry of Postal, Telecommunication and Courier Services	5
	TOTAL	35

Source: Researcher, 2020

1.13.6 Sampling Method

In this study, stratified random sampling of selecting the respondents was ideal.[69] This is achieved by dividing the respondents into their respective units, areas of functions and departments. Random sampling was used to select the actual participants based on the representation size of the created subgroups.[70] The method is applicable to all the various types of population units as it ensures that they are all represented. Bias in the sampling was minimised or eliminated as it presented adverse

[69]Ibid, p 46.
[70]Op Cit.

outcomes of the response.[71]

1.13.7 Validity and Reliability of Data Collection Instruments

To ascertain whether the content and validity of the interview guides and questionnaires was appropriate and relevant to the study objectives, consultations with the supervisors and any relevant expert in this field of study was sought to help improve the quality. This helped in determining whether the tools answered the research questions. However, to ensure reliability of the research tools, the researcher administered the instruments to the targeted sample in order to ascertain that only selected participants responded. This helped to avoid biasness of the tools.

1.13.8 Data Presentation and Analysis

The data that was collected through questionnaires, interviews, libraries and internet was analysed using descriptive statistics and inferential calculations.[72] Interpretive content analysis and inferential statistics was used in coming up with the research findings. From interpretation, the study was able to draw conclusions and make recommendations.

1.13.9 Ethical Considerations

Informed consent is the most important ethical aspect that guides a research. Participants were briefed on the purpose of the study and relevant authority and documents were sought. This ensured that the respondents provided accurate

[71]Bryman, A. (2012). *Social Research Methods,* 4th Ed. Oxford: Oxford University Press. pp. 186-187.
[72]Mugenda, A.G. (2011). *Social Science Research, Theory and Principles.* Nairobi: Applied Research & Training Services.

information without fear.[73]

1.13.10 Scope of the Study

The study reposed on the national security in Kenya and Zimbabwe in relation to the emerging cyber security threats. The study focused on the assessments of the cyber defence mechanisms and strategies in the two states in regard to these threats. The population of the study was drawn from different departments, ministries and institutions in the two states.

1.14 Chapter Outline

This project is structured into five chapters with an introduction and conclusion of the themes discussed in every chapter. **Chapter One** outlined the background of the study, statement of the problem, literature review and research hypotheses, and significance of the study as well as the research questions and objectives. **Chapter Two** presented the legal frameworks put in place for the two (Kenya and Zimbabwe) countries to respond to cyber security threats.

Chapter Three assessed the cyber security defence strategies available in both countries (Kenya and Zimbabwe). **Chapter Four** sought to determine the regional cyber security defence strategies incorporated by the two countries. **Chapter Five** presented the summary of the key findings, conclusions and recommendations.

[73] Marianna, M. (2011). What are the Major Ethical Issues in Conducting Research? Is there a Conflict between the Research Ethics and the Nature of Nursing?. *Department of Nursing Health Science Journal*, 5(2), 3-15

CHAPTER TWO

LEGAL FRAMEWORKS PUT IN PLACE IN KENYA AND ZIMBABWE TORESPOND TO CYBER SECURITY THREATS

2.0 Introduction

The chapter presents the response rate of the study, a brief description of the demographic characteristics and the findings. It begins by explaining the Development of the Cyberspace in Kenya and Zimbabwe. Goes further to discuss Kenya and Zimbabwe cyber legal frameworks, the rules and regulations and how they govern the cyberspace operations in the regions.

2.1 Response Rate

This research utilised primary data in comprehending the cyber security threats which Kenya and Zimbabwe faces and the presentation is given below as follows. The study targeted 70 people from both countries each having 35 respondents. Out of these, 60 were to participate by filling in the questionnaires while 10 were to be interviewed. In this regard, 60 questionnaires were issued to the study participants. From these, 58 were returned. 5 persons were interviewed. This made a response rate of 98.2% which was deemed sufficient for analysis.

Table 2.1 Response Rate

Questionnaires Issued	Questionnaires returned	Response Rate
70	58	98.20%

Source: Field Data, 2018

2.2 Demographic Characteristics

2.2.1 Gender of Respondents

As regards to gender, it was established that, 46 respondents representing least 66.7% of the sample size responded to the questionnaires, with the majority of the respondents being males (70%) while females accounted for 30% of the total respondents as shown.

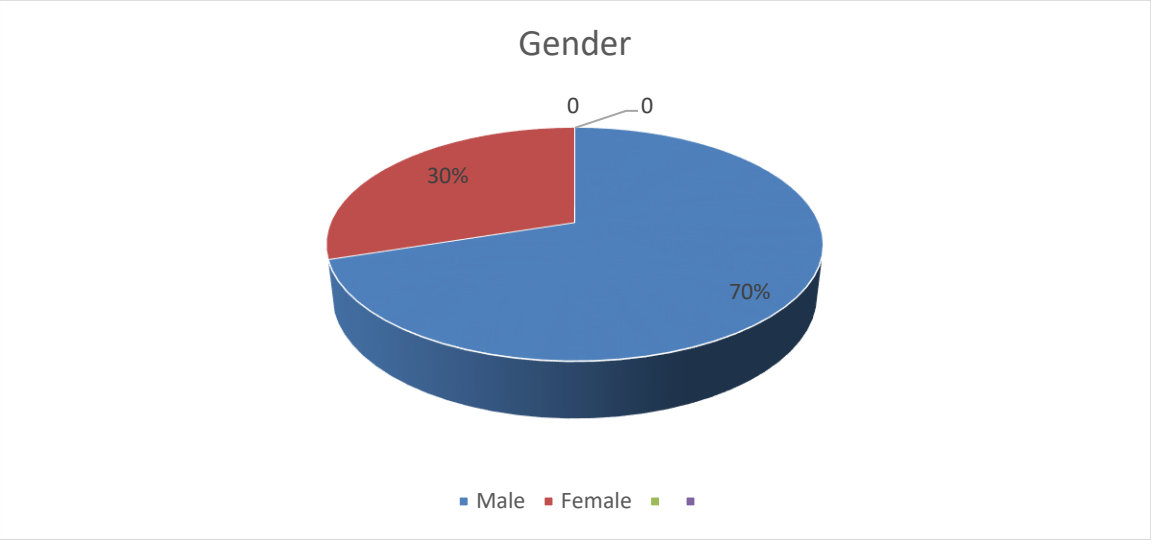

Figure 2.1: Genders of the Respondents

Source: Field Data, 2020

From the figure above, the proportion of male respondents was higher than that of female due to high involvement of men in cyber security initiatives at the national level. More males than females were well versed with cyber security threats and solutions than females.

2.2.2 Age of Respondents

The age distribution was a critical component which entailed this research. Majority of the respondents were 36-50 years of age, while on the other hand minority was above 65 years of age and above. The explanation for such distribution variation

can be attributed to digital literacy among the youthful people, who have recently completed school and attained employment in ICT related sectors. However, those in the higher age bracket are not technologically savvy and know very little concerning cyber security. The age distribution is as shown in the chart below.

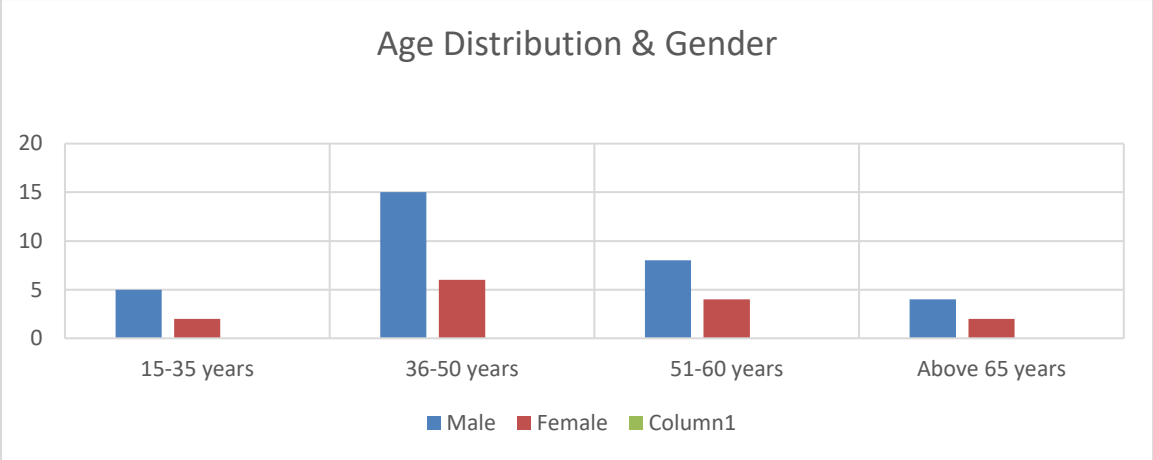

Figure 2.2: Age Distribution

Source: Field Data, 2020

2.2.3 Level of Education of Respondents

Majority of the participants had acquired University education, representing 58% of the respondents, while 32% of the respondents had acquired secondary (as well as College Level) education. The rest of the respondents had either higher qualifications such as, masters Degrees and PhDs which were classified as others in this research as shown in the figure 2.3. Majority of the respondents had University education and expert knowledge about cyber security in developing countries. The level of education greatly influenced the worthiness of their opinions and informed this research, on the thematic areas of concern which constituted the knowledge gap.

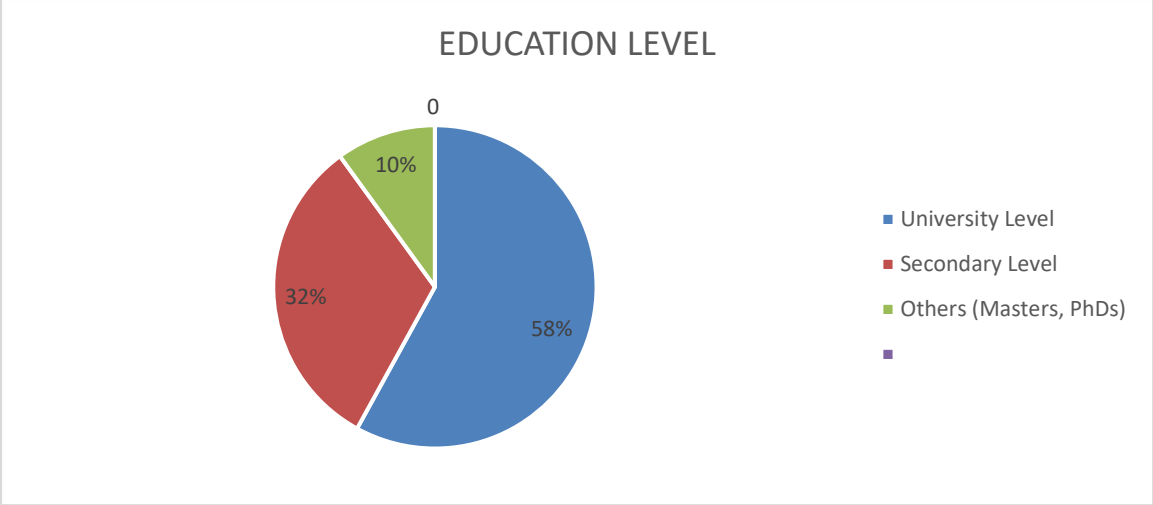

Figure 2.3: Education Level

Source: Field Data, 2020

2.2.4 Marital Status of Respondents

Although not being of great importance to this research, most of the participants were married at (32.6%) while single respondents were 26%, separated constituted 21.7% and divorced represented 19.5% of the respondents as shown.

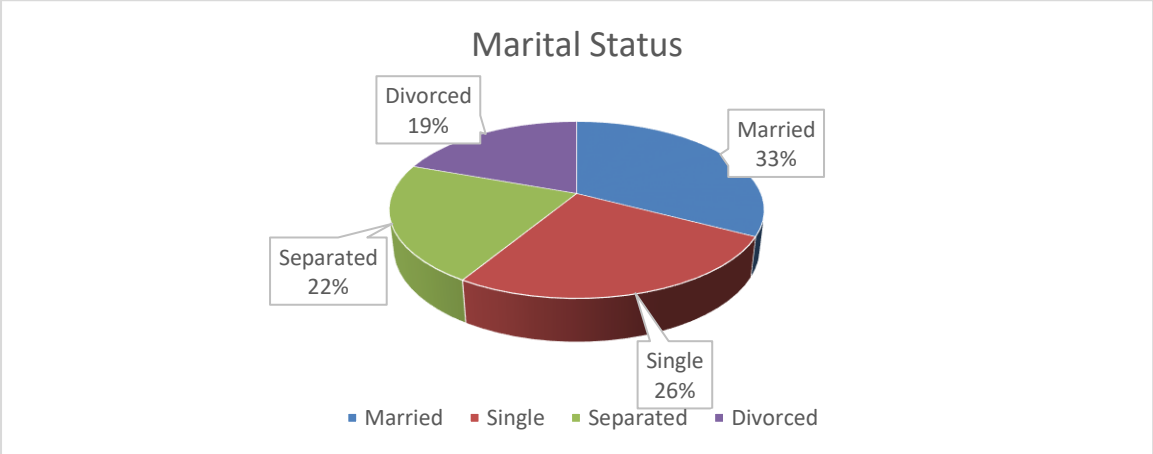

Figure 2.4: Marital status

Source: Field Data, 2020

The above statistics reveal that majority were family people with families.

Additionally, majority of the respondents were in formal employment constituting 91.3% of the total respondents, while 8.7% were self-employed. While occupationally the respondents differed from one another, they had extensive knowledge of the subject under study and constituted rich informant's suitable for this research study.

2.2.5 Occupation of the Respondents

The research probed further to establish the nature of the work done by the respondents and established that, they ranged from being businessmen to security operators, while others were centre analyst, cyber security analyst officers as well as legal liaison officers also participated in provision of data. Others were public officers and heads of information department in Government offices.

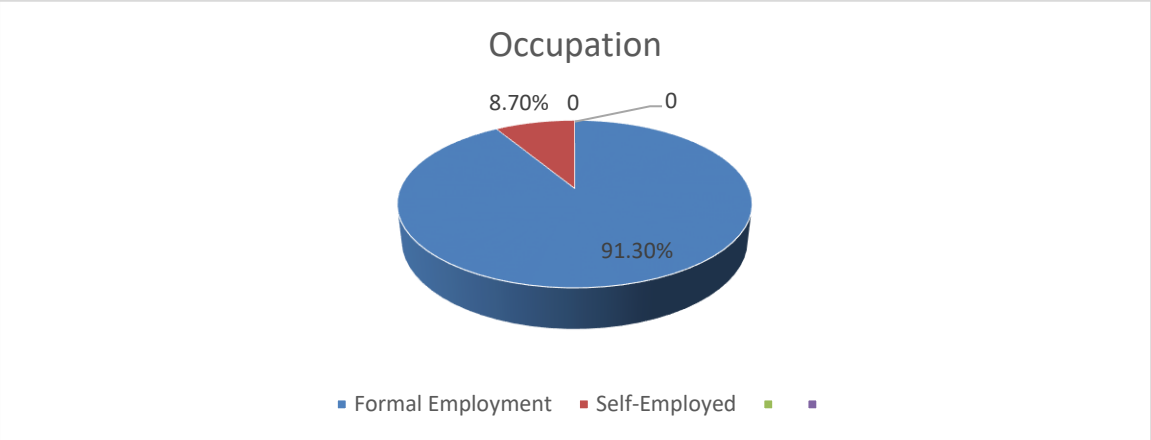

Figure 2.5: Occupation of the Respondents

Source: Field Data, 2020

2.3 Definition of the cyberspace, cyber security and vulnerabilities

Cyber space involves all the digital assets and platforms which are connected to form virtual ground which is the cyber space. This starts from digital devices such as mobile phones, telecommunication gadgets, computer software's and hardware's. Cyber security refers to efforts aimed at safeguarding the cyberspace environment and

its users from all threats that might threaten their security as well as that of the nation.[74] Cyber security can be realised only if the critical ICT infrastructure of any state is safe guarded from its destruction.

Critical national infrastructure constitute part of the new dynamic shift in the national security from the traditional security that, centred on the state to the one that views the main five sectors above, as key to the survival of the states.[75] However, security is called for where there is insecurity. Insecurity is the inherent, threats to a system, organisation or state.[76] Cyber insecurity is therefore, the exposure of the cyberspace to the vulnerabilities inherent in the cyber realm.

The researcher enquired from the respondents on what they understood by cyber security, and established similar sentiments where respondents stated that;

"*Cyber security is the security of the cyberspace and ensuring internet users do so safely and are protected from online crimes"*.

Additionally, another respondent stipulated that;

"*Cyber security is Practice of ensuring confidentiality, integrity and availability of information among internet users"*.

In totality, cyber security is protection of anything connected to the internet i.e. hardware and software. The development of these ICT technologies and infrastructure expanded the cyberspace and equally made it to become a critical component of the state's virtual territory and ground. It is noted that, vulnerabilities became also prevalent in the cyberspace, as it graduated to an operation theatre. The main components of the threats became the software. In fact, the software downloaded in one country and reinstalled in other countries can be tempered with

[74] Kabanda,G. (2020). *A Cyber security Culture Framework and Its Impact on Zimbabwean Organizations*. Honolulu, Hawaii: Atlantic International University

[75]Barry, B., &Little,R.(2000). *International Systems in World History: Remaking the Study of International Relations,* 1st Ed. Oxford: Oxford University Press

[76] Ibid,

and illegally used to conduct cybercrime.[77] Therefore, there is the need of laws, regulations and international cooperation to maintain or attain cyber security.

2.4 The Kenya Cyberspace

The majority of countries in the Africa region began to realise that, their economic functions were through ICT as from 1997. ICT remained significant in the economy of Kenya and more pronounced from 2000.[78] However, from 2004, Kenya's ICT economy had not developed into a single entity. It was still characterised by fragmented institutions which were complimented by fragmented legislative acts that promulgated them. Kenya is placed amongst the leading ICT giants in Africa and thus having an economy of US$5.6bn.[79] In fact, this was a significant growth in both technologies and infrastructure. It should be noted that 31% of Kenya's economy is on the electronic platforms with Mpesa leading the pack.[80]

According to Kneedler (the Deputy Chief of the Mission, at US Embassy in Nairobi, Kenya), who states that,

"Kenya is a key partner and ally of the US and a leader in cyber security in Africa. We are pleased to collaborate with our Kenyan partners on this important initiative to help secure networks and protect cyber space across the continent. So these are the efforts of Kenya to protect cyber space across the continent. So these are the efforts of Kenya to safeguard their cyber environment".

This is notable concern of the multidimensional approach to increase cyber security space by Kenya and USA. Kenya's national critical infrastructure starts from the satellite links, undersea cables joining at Mombasa, the great fiber linkage from Mombasa to Nairobi. It eventually has its tentacles spreading internally, favouring the most concentrated Southern and Western parts of the country. These undersea cables

[77] Wei, S. et al. (2010). *Superficial simplicity of the 2010 El Mayor–Cucapah earthquake of Baja California in Mexico.* Pasadena, California : California Institute of Technology
[78] Brencil, K. (2018). Kenya Cyber Security Report 2018. Nairobi: SERIANU Publication
[79]Ibid, p 35.
[80]Ibid, p 37.

provisions are mainly from the WACS, EASSy and SEACOM.[81] The internal has public safety and termini security at the road, air and sea ports. It includes the main highway surveillance and key installations, buildings and business hubs through the closed circuit television systems (CCTV). This is illustrated in the figure 2.1 below.

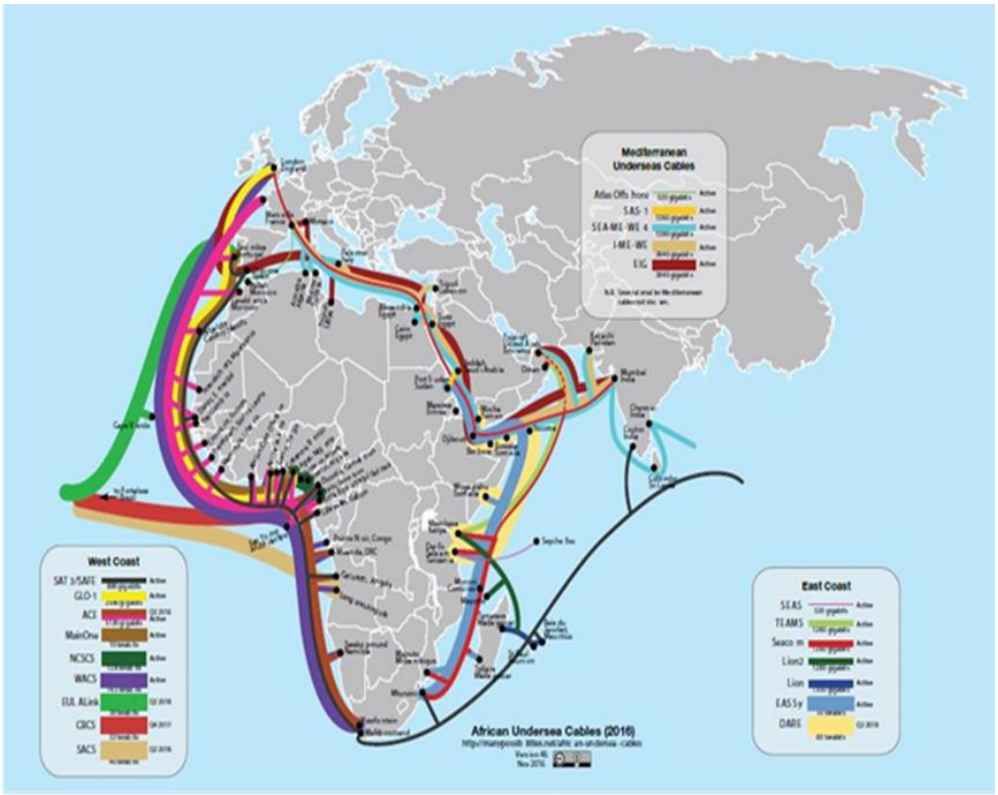

Figure 2.6 Undersea cables provisions

Source: African Undersea Cables

Cyberspace also includes the six interior components which are hardware, software, data storages, people, documentations and supplies.[82] Kenya's economy, society, polity, military and environment management are now dependent on the computers and relevant network systems. This is another dimension where the national cyber space scope is expanded. See also figure below

[81]Op Cit
[82] Douwe, K. (2011). *The definition of cyber security*. Oxford: University of Oxford

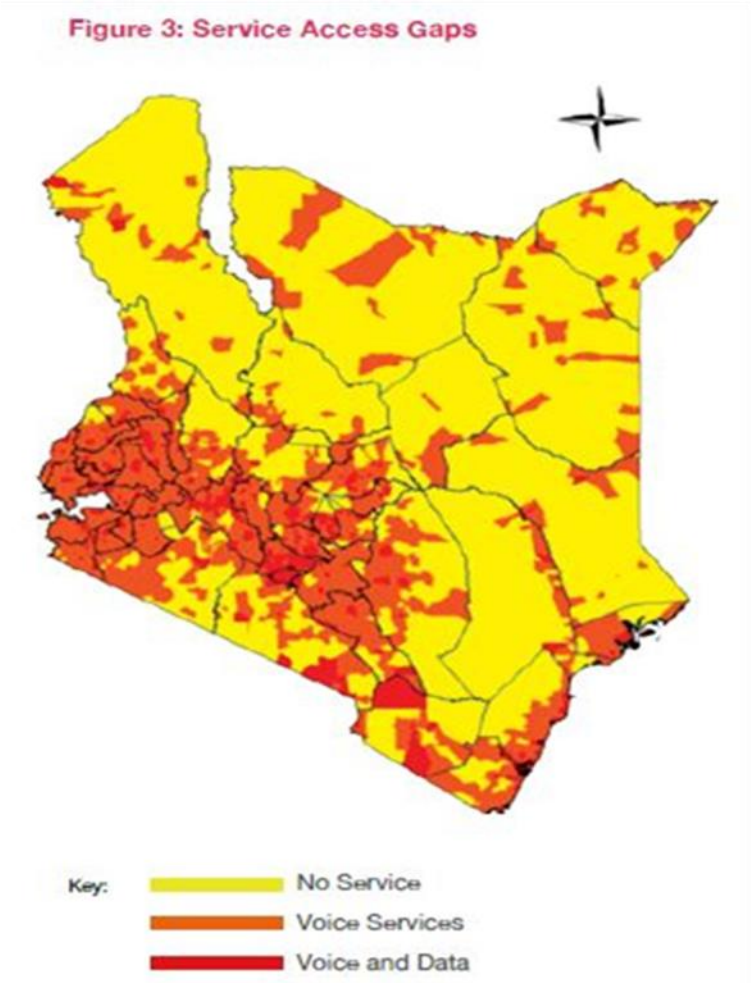

Figure 2.7 Service Access Gaps

Source: Kenya Digital Economy, 2019

Kenya further began developments of the ICT hubs such as the Lab Africa and NaiLab as the major laboratories. This attracted major global players in ICT, as they sought partnership with either local entrepreneurs or local institutes of higher learning.[83] Apparently this brought about another dimension of the cyber security threats as more adventurous youth are now participating in the hubs, posing a challenge to the Kenya national security.

[83]Brencil, K. (2018). *Kenya Cyber Security Report 2018*. Nairobi: SERIANU Publication

2.5 The Zimbabwe Cyberspace

Zimbabwe is among the developing states that have embraced the usage of knowledge and equipment of the ICT since 1999. The advent of the ICT witnessed penetration of the internet intensifying to 55.4% by early 2018.[84] Zimbabwe lags behind in regards to the inculcation of the principles of cyber security in the country at large, despite adoption of the ICT. The cyber space comprise of the linkages from the undersea cables that comes through the fiber from Mozambique, South Africa, Botswana as it passes from Namibia.[85] These undersea cables provisions are mainly from the WACS, EASSy and SEACOM as indicated in figure 2.1 above. The internal infrastructure comprises of the banking platform mainly the ZimSwitch, the telephone networks mainly the cellphones and the fixed landlines as well as fiber loops that are mainly on the commercial and cities with hives of internet activities. Both the undersea optical fiber connections for Zimbabwe are shown in Figure 2.3.

In the intervening time, statistics demonstrate that, under some rational uncertainty, the Zimbabwean economy is firmly becoming an internet hub and as the digital gap is closing, the growth of the economy is also witnessed. This upsurge in internet penetration and electronic transactions presents that, computers are fast becoming accessories for committing crime.[86]

[84] POTRAZ. (2018). Post *and Telecommunications Regulatory Authority in Zimbabwe Report*. Accessed on https://www.itu.int/en/ITU-D/Conferences/GSR/2019/Documents/Zimbabwe_Contribution-GSR-19.pdf
[85]Veritas. (2019). *Zimbabwe National Policy for ICT 2016-2020*. Harare, Zimbabwe
[86]Kabanda,G. (2020). *A Cyber security Culture Framework and Its Impact on Zimbabwean Organizations*. Honolulu, Hawaii: Atlantic International University

Map 12.2. Existing and Proposed Fiber Optic Network of Zimbabwe

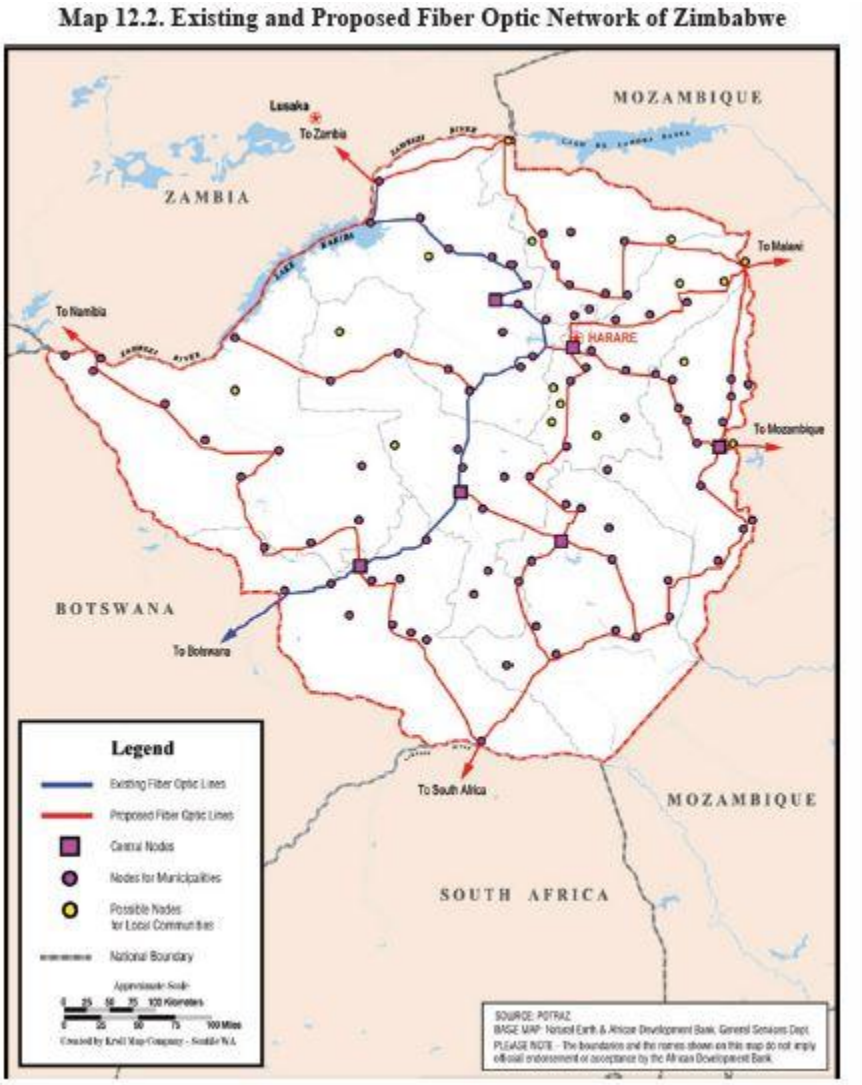

Figure 2.8Existing and Proposed Fiber Optic Network of Zimbabwe

Source: POTRAZ, 2016

It's estimated that, Zimbabwe's US$ 3, 6 billion comes from the electronic platform with Econet leading the pack.[87] Zimbabwe has to come up with a context of the legal frameworks that are ideal to the obtaining cyber security requirements. Further, it's estimated that 978 million people in 20 countries were exposed to cybercrime in 2017 and Zimbabwe is not an exception. Zimbabwe's public safety and security systems are apparently in the road, rail and air ports including ports of entries

[87]POTRAZ. (2018). Post *and Telecommunications Regulatory Authority in Zimbabwe Report*. Accessed on https://www.itu.int/en/ITU-D/Conferences/GSR/2019/Documents/Zimbabwe_Contribution-GSR-19.pdf

at the borders.[88] As such, the infrastructure is still limited mainly to transactional lines.

2.6 The Nexus between National Security and Cyber Security

In Kenya, cyber security has evolved to provide public safety systems, diverse economic activities and other systems in the government and the military. The cyber space needs to be securitised in order to benefit all the citizens.[89] This process leads to integration of cyber security into national security. The political realm remains to handle issues that challenge the cyber space.[90] Further, lack of cyber security society in the state exposes the economy, society and the state itself.[91]

From the military dimension, the states depended on the network systems in order to establish critical infrastructures and source or procure even weapons from different sources. However, the military sectors embarked on missions to identify the offenders of these cyber threats who were posing threats by leaking important government information.[92] It adopted both defensive and offensive capabilities for action within the cyber space, which indicate the beginning of cyber warfare capabilities being built in each and every state. Therefore, analysts of the developments in the cyber space have since concluded that, the cyber space was a fourth domain of warfare after the land, sea and air. Generally, all the state's facets for their survival are now dependent on the cyber space.

The researcher sought to establish the how "cyber security is part of national security". The respondents indicated that, cyber security is part and parcel of national

[88] Kabanda,G. (2020). *A Cyber security Culture Framework and Its Impact on Zimbabwean Organizations*. Honolulu, Hawaii: Atlantic International University
[89] Boulanin. V. (2017). *The development and discussion on LAWS Chapter*. Oxford: Oxford University Press
[90]Ibid, p 219.
[91] Hansen,.L., & Nissenbaum, H. (2009). *Digital Disaster, Cyber Security, and the Copenhagen School.* New York: New York University
[92]Op cit, 246.

security architecture which translates to an important asset of national importance. One respondent, asserted that,

"*Cyber security ensures that citizens can access government services in a safe environment, which does not compromise on their confidentiality and quality of data".*

Additionally, cyber security ensures citizens are able to access banking information in real time, without it being compromised by cyber criminals. Therefore, cyber security promotes trust and confidence among the population, which in essence steers economic growth and confidence among the users. This is achieved through security of sensitive data, which ensures national sovereignty is not compromised and both the national socio-economic and political wellness of a country is maintained.

It has become a matter of national concern which has transformed from traditional use of force (military sense), once the state's facets of survival are dependent on the cyber space. It is important that, the national security in Kenya and Zimbabwe has evolved and hence has the contemporary dimension to society, economy, political, environment and military.[93] The contemporary security as after the attack of institutions in 2007 in Estonia, other EU countries including the NATO integrated the cyber security policy into the national security and began to build cyber defenses for their cyber spaces.[94] These cyber defenses resultantly were then placed under the cyber defense management. This further enabled the establishment of the regional (CCDCOE) in Tallinn and Estonia in 2008. The USA under Barrack Obama leadership came up with the US Cyber Command (US Cyber Command) supported by Cyber Severity Strategy.[95]

---

[93] Dunn, T.A.(2008). *Imaging second messenger dynamics in developing neural circuits.*Rockville Pike: National Center for Biotechnology Information

[94] Landler, M., & Markoff, J.(2007). *Digital Fears Emerge After Data Siege in Estonia.* New York:The New York Times Company

[95] Perloth.N,(2012). *In Cyber-attack on Saudi Firm, U.S. Sees Iran Firing Back. Available at* https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

The alleged US cyber weapon, the Stuxnet, a virus developed for attacking Iran nuclear effort, brought a raw definition of national security for being affected by cyber weapons and cyber welfare.[96] The mainly suspected countries that have the capabilities of the cyber warfare are China, Iran, Israel, Russia and USA. Cyber-attacks affected USA national security leading to formulation of bills to deal with cyber security cooperation such, as the Cyber Information Sharing Bill, USA (CTIIC) and the T-AJCCC with the UK government.[97] Obama asserts that "the combination of cyber espionage campaigns against the military and all sectors, the potential loss of technological competitive edge, the low cost asymmetric warfare capabilities of adversaries and attacks on government, institutions indicate a session of national security".[98]

USA has grown to be the biggest nation that is allocating the national budget to cyber security efforts with support from the private and public sectors. The cyber security bazaar was estimated to grow to around US$120bn by 2012.[99] However, with this projection it can be anticipated to have grown to nearly US$130Bn. The capacity to spend such a huge budget on cyber defenses indicates a growth in the USA's new dimensions of conceptualising of the national security.

National security evolved to include human security which is essential and a matter of national agenda to most of the states. Majority of states have reconsidered their focus on security from the traditional military sense because of the cybercrimes which poses a threat to the national security. As such, national security has evolved and now encompasses human security. Conclusively, any attempt to reconsider

[96]Maslennikov, D. (2012). *Kaspersky Security Bulletin 2012.The overall statistics for 2012. Available at* https://securelist.com/kaspersky-security-bulletin-2012-the-overall-statistics-for-2012/36703/
[97], Finklea, M. et al. (2015). *Cyber Intrusion into U.S. Office of Personnel Management: Congressional Report*. Library of Congress. Washington DC,: Congressional Research Service
[98]Ibid, p 15.
[99] Op Cit

national security must factor in human security, which includes the individual, property, state, region and the global setting in international security.

2.7 Kenya's Geographical Position and Communication Networks in EAC

Kenya is a member of EAC and links different countries who are also its neighbours from South, North, East and West. They include Uganda, Burundi, Rwanda, South Sudan and Tanzania. In the same vein, Kenya provides communication link from the sea to the same countries. It therefore, stands as an economic and communication network in EAC. Africa cyber space particularly the undersea cables passes through Kenya especially through Mombasa. The undersea cable linkages include those of the TEAMS, SEACON, LION 2 and EASSy. However, with the volatile security situation in Somalia, the Kismayo and Mogadishu terminal points are more prone to attacks and have become less used especially the former in the northern coastal line town of Kenya.

The undersea cables connect Kenya to the Mediterranean undersea cables then to all other countries globally. There is also the radio and data links which are inland and proceed to all parts of Africa. The networks again pass through the Mombasa port to Nairobi and to the inland states of the EAC and IGAD countries. In additional, Kenya reviewed the NOFBI in order to improve and expand the network as well as expand the national critical infrastructure in the telecommunication.

2.8 Legal Frameworks in Kenya

The study sought to establish some of the legal frameworks, laws and instructions available in the country for regulating cyber security. Some of the legal frameworks established from the respondents included; "the Penal Code, Kenya

Communication and information (Amendment Act Cap 411)". Other notable cyber security legislations in the country included; "the Data protection Act (2019) and computer misuse and cybercrimes Act (2018)". The respondents also acknowledged the various national institutions engaged in cyber security pointing, at the Ministry of ICT, MICNG as well as CAK.

The principal document for structuring all the legal frameworks of a state is the constitution. Thus, all other subsequent legislature efforts will be in the spirit of the constitution.[100] The Constitution of Kenya, Chapter 14, acknowledges protection of the nation from all threats. Hence, it is certainly that, the constitution is observant of the dynamics in national security. Since security has evolved to include the societal, economics, military, political and environment to be essential parts of national security.

There is evidence of commitment to integrate both the traditional and modern notions of security into national security. The national interests are almost the same in all countries regionally. The organisations which are duly responsible for national security are the (KDF), the (NIS) and the (NPS). Their existence is provided by articles and chapters in the constitution.

All the security organisations are created through the legislative laws of the state in line with the Constitution of Kenya for the provision of the defence and security services as public goods to the nation.[101] KDF is created by Chapter 99 of the Constitution of Kenya. The subsequent section 3(3) empowers the president in consultation with the DC to form and promulgate any establishment inconformity to any perceived threat. The president once advised by the DC can formulate any unit in KDF to address the pertinent threat as observed in national security of the state of

[100]Gok. (2010). *the Constitution of Kenya 2010*. Nairobi: Government Press
[101]Barry, B., &Little,R.(2000). *International Systems in World History: Remaking the Study of International Relations,* 1st Ed. Oxford: Oxford University Press

Kenya.

The PNS is formed and commanded through Chapter 84 of the Constitution of Kenya, 2014 and Articles 243-245. The Constitution empowers the NPS to enhance law and order in the country and advising the (NSC). So the NPS once observant of any threats to the national security in whatever form has the mandate to inform the NSC. The NIS is formed through the Kenya CAP 2012 as jointly with the National Security Act 2014. These are in tandem with Articles 239(6) and 242(2) of the Constitution of Kenya. All these laws are there to enable the security apparatus to enhance national security.

The Computer Misuse and Cyber Crime Act of 2018, pronounces the crime in the republic of Kenya.[102] The act is administered under the main criminal offences in the state by the NPS to enable its reinforcement. The Kenya Information and Communication Act, 2019 has provisions for the formulation of institutions such as the (CAK) mandated to come up with a cyber-security management frame work.[103] The same CAP has the enhancement in the provisions to address cybercrimes. It has tried to look at the international best practices. It covers the full array of ICT and enhanced cyber ecosystem in the republic of Kenya. Though, it may appear to be quite encompassing it runs short of prescribing these acts where they would escalate from being criminal act to be aggressive acts of a hostile organisation or state both as an internal or external influence, the act of war.

Kenya's former Post and Telecommunication Corporation was split into separate entities in 1999, the PCK and TK which was eventually privatised. The (CCK) became the regulation body of the telecommunication industry. The (NCS)

[102]Gok. (2018). *the Kenya Gazette Supplement Act. Nairobi*: Government Press
[103]Gok. (2019). *the Kenya Information and Communication Act*. Nairobi: Government Press

became responsible for policy and final Appeal Tribunal for arbitration.[104] It should be noted that, in Kenya the ICT falls under a host of legislature pieces that cater across the diverse industry. The pieces of legislature include the Kenya Broadcasting Act (KBC, 1988) revised to become the Kenya KBC 2014.[105] The original KCA Act of 1998 became the KIC (Amendment) Act 2013 (41a). The same Act was further amended in 2019 as to incorporate the main definitions of the cyber security and space.

In this regard, "Kenya's cyber security regulation" and auspices fall under Ministry of ICT, the CAK originally the CCK including the Kenya ICT Authority. Though these institutions are overseeing the ICT, they lack the constitutional purview of the national security as stated in the Kenyan Constitution. In fact, the purview is concerned with ICT security packages, their installation, licensing and its authorisation of the purchases and distribution in the country.[106] The national security integration of the cyber security as defined by the Constitution of Kenya is not identified and addressed in the components of these pieces of the legislature.

The constitution takes account of the protection against internal or external threats in Kenya. What all these legislature pieces are creating is the critical infrastructure that then forms the cyber space. The cyber space is a virtual ground which should be acknowledged as the fourth domain of warfare for Kenya as it has the land, air and sea. It is very certain that, cyber security has evolved such that, the state of Kenya is equally threatened through cyber insecurity like any other state in the international security system.

2.9 The legal frameworks in Zimbabwe

[104]GoK. (2014). *Kenya Broadcasting Corporation Act*. Nairobi: Government Press
[105] Ibid, p 22
[106]Ibid, p 11.

Crimes associated with the cyber space are dealt with using the "Zimbabwe Constitution of 2013, the CL (Codification and Reform) Act, Chapter 9:23".[107] The government passed Bills to combat these threats which include: "the Computer Crime and Cyber Crime Bill, Data Protection Bill as well as Electronic Transactions and Electronic Commerce Bill. The Zimbabwe National ICT Policy 2015", formed part of the regulating framework. Further, the Zimbabwe Republic Police, National Intelligence Services and the Defence forces Acts formed part of the legislative laws governing the cyber security.[108]

The Zimbabwe's Constitution of 2013 observes under Article 207(1) the (ZDF), (ZRP), (NIS), (ZPCS) and any other service established through Acts of parliament. The ZDF is created by Chapter 11:02 (1) (b) in Article 211 of the Zimbabwe Defence Act, which provides the functions of the defense forces. In reference to the ZDF Act, 11:02, upon agreeing with the CDF, the Minister of Defence may form and name a unit to deal with the threats to national security. It therefore, implies that the aspect of the involution of national security to include the cyber security can be addressed by formulation of a competent formation or unit to deal with the cyber security threats. ZRP was formed through the Article 219 of the Constitution with functions spelt in Article 211(1).[109] It is very cognisant of the ZRP efforts on enhancing protection of the national security and interests through cooperation with other security services. The ministers responsible for safeguarding the security of the nation have the right and power to respond to national security when necessary. This implies that both of them can have units responsible for managing the cyberspace.

The Public Order and Security Act, also pronounces cybercrimes and related

[107] GoZ. (2013). *the Constitution of Zimbabwe Act no 20*. Harare: Government Press
[108]Ibid, p 89.
[109]Op cit, p 93.

offences. It's also bent towards coming up with measures of the cyber damages to other individuals and the states. It tends to have a gap with Article 62(1) which allows everyone access to information in Zimbabwe.[110]

The main Ministries responsible for the governance of the cyber space activities are the Ministry of ICT and Cyber Security and the Ministry of Postal, Telecommunications and Courier Services. Further, the Ministry of Postal, Telecommunications and Courier Services forms the POTRAZ, which regulates the implementation of ICT hardware, software and the relevant applications. It also allocates bandwidths and frequency assignments to the respective actors in the industry.[111] The services of the telecommunications networks and systems in the industry are regulated through the Interception of Communication Act (2007). More so, the Criminal Code (Codification and Reforms Act), Chapter VIII (162-168), do not have any power to incriminate any cyber war actions, except to invoke other sections of the Security Acts.[112]

Further, the researcher sought to establish the effectiveness of the legal frameworks laws and regulations in managing cyber security. According to respondents,

"The effectiveness of these frameworks cannot be evaluated, since they were enacted recently and their operationalisation is ongoing. Other respondents posited that, these legal frameworks are sufficient and effective in deterrence of cyber threats, since they encompass all what is required to ensure the safety of cyber systems".

More emphasis was laid on the effectiveness of the frameworks in regulating unmanned aerial vehicles. Other respondents asserted that,

"The legal frameworks been effective in ensuring greater cooperation with relevant organisations, locally and internationally thus ensuring performance at

[110]Op cit p 95.
[111] GoZ. (2000). *The Postal and telecommunication Act of Zimbabwe, chapter 12.* Harare: Government Press
[112] GoZ. (2006). *The Criminal Code (Codification and Reforms Act), Chapter 9:23*. Harare: Government Press

reduced costs".

The effectiveness of the laid down legal frameworks in regulating cyber security was attributed to the transparency with which the government has been accorded. The delivery of government services has been improved greatly and securely, due to the enactment of various legislations which safeguard the usability and management of information therein.

The institutional and legal frameworks established to prevent cyber-crimes in the country are subject to routine upgrades, due to sophistication of technological advancements and the complexity with which digital world is advancing. Whereas, the legal frameworks and regulations are not limited, the advancement in technology has warranted internet users, to upgrade their security apparatus, due to improvement in current threats which face internet consumption. There is an urgent need for national cyber security capacities to be upgraded to meet the current demands of the cyber space.

2.10 Chapter Summary

Cyber security threats pose risks to the national security of majority of the states including Kenya and Zimbabwe as they seek to invest and enhance their ICT capabilities and infrastructures. There exist a number of legislative tools available in both countries, which facilitate attainment of cyber security as discussed above. Though, Zimbabwe has drafted various Bills and Acts aimed at curbing this menace, it lacks a comprehensive Cyber security framework anchored in law. Therefore, it is of great importance to develop an effective national Cyber security legislation that will combat cyber insecurity which poses a great threat to strategic government information leading to devastating impacts that affects the economy posing great

threats to the national security. The devastating effects of these threats have been experienced in all countries worldwide including Kenya and Zimbabwe.

CHAPTER THREE

CYBER DEFENSES AVAILABLE IN KENYA AND ZIMBABWE TO COUNTER CYBER SECURITY THREATS

3.0 Introduction

The chapter begins by defining the state institutions available for responding to cyber threats. The distinctions of the cyber security and cyber space were also discussed and their differences brought to the fore. This included their mechanisms and implementation. The implementation however, was discussed under the GDT. The theory prescribed ways and conditions of assessing the cyber environment and the applied relative defence mechanisms. The chapter also discussed the findings on cyber institutional frameworks in both countries before giving the belvedere of Chapter Four.

3.1 Definition of the state institutions

Institutions are laws and policies that guide an establishment in a state.[113] The established organisations and their boards then make the states administrations functional. Since the states are concerned with the existence of anarchy both internally and externally, they are assured due to existence of the institutions of having no chaos internally. However, institutions are occasionally mixed up with establishments. The establishments follow the structures availed by the legal institutions for establishing organisations.

Organisations exist by institutional frameworks and in turn shape institutional requirements of the states. Therefore, institutions are standards, techniques,

[113] Douglass, N. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press

agreements and ethnicities that are part of the state response.

3.2 The Cyber Security and Cyber Defence Institutions

The building blocks for an effective cyber security and defence ecosystem are the states' institutions countering the rising of threats relevant to the progressive inventions within the cyber purview.[114] With the challenges in many states that, the cyber space is dominated and spearheaded in its development by the private sector, even though the states avail the necessary funding and bearing, governing authority remain challenged for the security of the cyber space. States' systems are demarcated in the cyberspace relative to contemporary progresses in the ICT development. The cyber space is dominated by the non-state actors.[115]

The customary apparatuses aimed at stalking events happening in the real ecosphere, data, criterions and capacities remain routinely unbeneficial as to the "virtual' tracings or complements. Therefore, the environment of the virtual is now challenging the physical environment.[116] The threats often acknowledged afterwards are slightly pursued whilst before or in process. In the cyber space, early warning system, early signals of a cyber threat need to be in place managed by designated institutions.[117]

The comprehensive institutional realm offers point of departure for the cyber security ecosystem. The most prevalent ecosystem comprises of both actors in the national and international arena.[118] Other factors that may affect the cyberspace as

[114]Ibid, p 8.
[115]Acemoglu, D., & Robinson, J. (2012). *Why nations fail: The origins of power, prosperity and poverty*. New York: Crown Publishers
[116]Andrews, M. (2013). *The limits of institutional reform in development*. New York: Cambridge University Press.
[117]Walls, A., Perkins, E., & Weiss, J. (2013). *Definition: of Cyber security*. Stamford, Connecticut, United States:Gartner Inc
[118]Ibid, p 14.

parallel lines are the non-state actors, often with no clear obligations or holding the security and defence mechanism to enhance safety in the cyber space.

3.3 The State Cyber Security and Cyber Defence Mechanism

Cyber defence emphases on averting, perceiving and providing the appropriate reactions to threats on the national critical infrastructure.[119] As the evolution in capacity and complication in nefarious cyber activities increase, cyber defence becomes indispensable to safeguard the subtle national infrastructure, resident information and resources.

Cyber defence offers necessary guarantee to procedures and actions, unrestricted beginning from the fears. It is important to enhance the security strategy and reinforcement of institutions.[120] Cyber defence improves the security in critical institutions and their locations. Every state has the requirement to detect and react to vindictive actors on its systems. However, some states may not distinct cyber security and cyber-crime. These are distinct and complex and they necessitate defence planned to cater for their uniqueness, discretion and security repercussions.[121] Furthermore, a distinction must be given between cyber defence and cyber security, where the latter is about safeguarding computer networks. On the other hand, cyber-crime is defined as illegal actions on the computer networks perpetuated by unauthorised actors which threaten the human and nation security.

The accountability role of securing the state's critical infrastructure and managing the cyber security threats is mandated to state agencies and private organisations. Therefore, it is in their interest to cooperate mutually and adopt

[119].Ibid, p 15.
[120] Austin, G. (2012). The Cyber security: Shared Risks, Shared Responsibilities. *A Journal of Law and Policy for the Information* Society, 8 (2), 81-103
[121] Gustav, L. (2012). *Meeting the Cyber Security Challenge*. GCSP Geneva Papers-Research Series no. 7. Geneva, Switzerland

strategies that will help in managing of the threats. In developing cyber security defenses, priorities should be to protect the established institutions, come up with robust systems for the protection and detection in the cyber space with skilled manpower to respond to the threats of the national cyber ecosystems. However, in order to comprehend the cyber defence mechanisms, the general deterrence theory (GDT) is utilised.

3.4 Using the General Deterrence Theory (GDT) in Building Cyber Defenses

The GDT outlays the founding principle on the context of defending, protecting, deterring and the ultimate remedy. The theory empowers inspection of the necessary security procedures for effectively controlling the cyber environment.[122] However, there exist other prevalent theories in the cyber security studies. The GDT mainly focuses on countering the nefarious actions, how they relate and the consequence of the cyber security and defence mechanisms in the respective cyber defence institutions.

The GDT has four mechanisms which include deterrence, prevention, detection and remedy as shown in figure 3.1 below. The actors can equally be deterred from committing criminal cyber acts by using necessary procedures.[123]

[122] Alanezi, F.et al. (2014). *Combatting Online Fraud in Saudi Arabia Using General Deterrence Theory (GDT).*London: Brunel University

[123] Straub, W., & Welke, R. J. (1998). *Coping with systems risk: security planning models for management decision making*. Hong Kong: Management Information Systems, p 441-469.

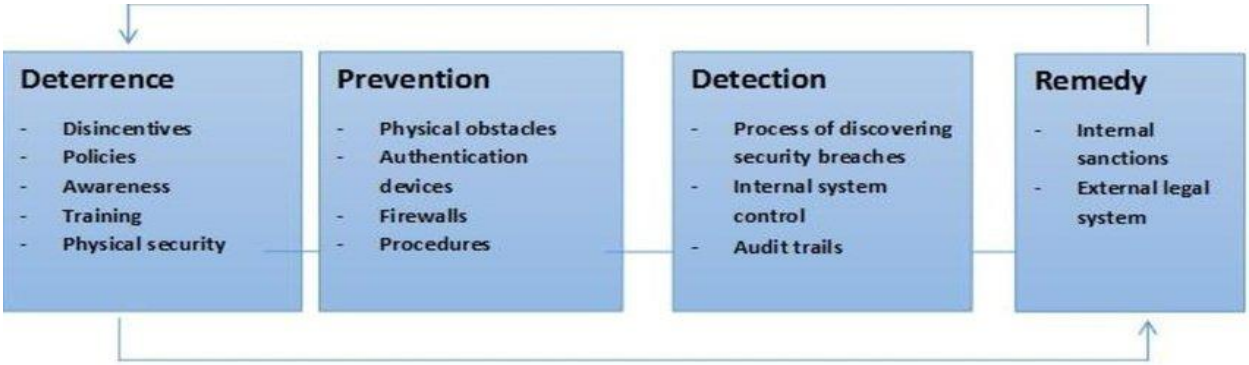

Figure 3.1: the GDT Model

Source: Alanezi et al, (2014)

3.5 The State Approach to Cyber Security

In approaching cyber security in a state, the public and private sectors are mainly concerned with the information security. The state is concerned with both the information security and the cyber security. Information security is part of the "cyber security" that deals with the security of the available information for storage, transmission or retrieval. The information security denotes to safeguarding of cyberspace activities and information.[124] The information must be found in its (CIA).

The integrity of the information implies to the safeguarding against inappropriate information alteration or obliteration and embraces guaranteeing information non-denial, accurateness and genuineness. The confidentiality component is the protecting of the sanctioned precincts on access and revelation, together with the resources for defending particular privacy and exclusive data. The third part is concerned with the availability of the information, which includes, guaranteeing appropriate and consistent right to use and the correct usage of the information.[125]

States are in a progressively problematic condition ever since they started

[124]Ibid, p 8.
[125]Buse, C.(2009). When you retire, does everything become Leisure? Information and Communication Technology Use and the Work/Leisure Boundary in Retirement'. *New Media and Society*, 11(7), 1143-61.

using the cyberspace. Ideally some have seen cyberspace as the virtual ground for conducting cyber warfare, impeding the opinion of entire disproportionateness. The disproportionateness is that asymmetry part of the cyber warfare.[126] The secretive and communal information arrangements are pounced on by even minor groups of experts in ICT using progressive replicated approaches. The dreaded encounters in cyber domain are the overwhelming cyber-attacks on the state's critical national infrastructure. It could be even worse if combined with kinetic or physical attacks.[127]

States are formulating computer systems procedures countering the adversary state's structures. The threat designed for disproportionate computer assaults are concerns of every state compared to susceptible noncombatant substructures. The ground of cyber security is everywhere information infrastructures are whether belonging to the private sector or government. Therefore there should be approaches to deal with emerging crises and partnership with different stakeholders and actors in both public and private sectors in an effort to respond to emerging cyber security threats.[128] As such, the state must strengthen state cyber competences, and then improve the resilience of the general structures of state cyber ecosystem.

The state must protect the cyber space and information even from the non-state actors both private and public companies and organisations. (NCSC) is mandated with protection of Kenya's cyber security. However, other state actors involved in investigating cybercrimes include CSIRT-Kenya and the iCSIRT under the auspices of the MICT. The main functions of the institutes are to identify, defend and salvage in combating cyber space threats and crimes. Threats are analysed and categorised in accordance to the laid down classifications adopted in Kenya. The

[126]Haddon, L., & Silverstone, R. (1992). *Information and Communication Technologies in the Home: The Case of Teleworking,* Working Paper 17. Falmer, Brighton BN1 9RH, United Kingdom: University of Sussex
[127]Ibid, p 34.
[128]Ibid, p 36.

institutions work in tandem with the security operations centre of the government, to produce new policies of protecting the cyber environment, threat evaluation, application and strengthening of the existing cyber defence mechanisms. There are also available mechanisms, procedures and policies for safeguarding these threats and response to cyber security incidents in Kenya.

3.6 The Institutional Frameworks in Zimbabwe

In Zimbabwe, cyber related crimes are dealt with through the judiciary system. The courts are part of the institutions that govern the cyber space. Zimbabwe's Constitution of 2013 and the CLCR Act, Chapter 9:23 empower the courts to handle such cases.[129] The Bills relating to cyber security and cybercrimes which were passed into law by the parliament, include; "the Computer Crime and Cyber Crime Bill, Data Protection Bill, Electronic Transactions and Electronic Commerce Bill". These Bills promote the establishment of structures that would be used to administer the cyber space. In addition, ZRP, NIS and the ZDF are part of the institution enforcing governance of the cyber security.[130]

ZDF is created by Chapter 11:02 (1) (b) of Zimbabwe Defence Act, through Article 211 which provides for the CDF and the Minister of Defence to deal with threats to national security. The evolution of national security to include cyber security can be addressed by security services' formation or unit to deal with the cyber security threats. The Article 203 of the Constitution formed the NSC mandated with formation of the NSP. The ministers responsible for these services have the right and power to respond to national security threats when necessary. This implies that the security service can have units responsible for managing the cyberspace.

[129] GoZ. (2013). the *Constitution of Zimbabwe Act no 20.* Harare: Government Press
[130]Ibid, p 89.

The main ministries responsible for the governance of the cyber space activities are the MICT, CS and MPTCS. The MPTCS also formed the (POTRAZ), which regulates implementation of ICT hardware, software and relevant applications. Further, it allocates bandwidths and frequency assignments to the respective actors in the industry.[131] The POTRAZ services the telecommunications networks and systems in the industry.[132]

The Zimbabwe ICT framework is composed of the MICT and Cyber Security transport and Communications, Media, Information and Publicity. The monitoring and implementation bodies include; POTRAZ, BAZ and the (MIC). The universal service fund and the Broadcasting Fund all contribute towards some identified Isolated and Disadvantaged Communities. The Funds raise their revenue from the subscriptions by members' contributions and commissions. There is interaction between the respective bodies as they execute their mandate.

"*The ITU has ranked Zimbabwe the second most dynamic country globally in one of three categories that measure the development of ICTs. The development is measured by what is called an ICT Development Index (IDI), which the ITU uses to determine the ICT readiness, the level of use of ICTs and the impact of the efficient use of ICT in a country*".

[131] GoZ. (2000). *The Postal and telecommunication Act of Zimbabwe, chapter 12*. Harare: Government Press
[132]GoZ. (2016*). the Statutory Instrument the Post and Telecommunications (Consumer Protection) Regulations*. Harare: Government Press

Most dynamic countries (top ten)

Change in IDI value (%)		
IDI rank 2011	Country	IDI % change
117	Ghana	23
115	Zimbabwe	19
68	Azerbaijan	15
88	Fiji	14
49	Kazakhstan	13
60	Brazil	13
47	Saudi Arabia	13
40	Bahrain	13
114	Kenya	12
73	Georgia	12

Figure 3.2 Most Dynamic Countries in ICT Development

Source ITU Report, 2012

The comparison of the leading country by ITU was conducted in 2012. It indicates the growth in the ICT industry where Kenya and Zimbabwe were recognised among the fastest growing ICT economies.

The researcher sought to establish cyber defense mechanisms that have been adopted in both countries to protect consumers of internet. Particularly, the researcher asked the respondents to rate cyber defence mechanism in the countries. The results indicated that, Kenya and Zimbabwe had invested in cyber security solutions that ensured that potential threats were addressed and mitigated appropriately. Majority of

the respondents agreed that, Kenya and Zimbabwe had taken appropriate measures aimed at mitigating the potential threats of cyber systems. Some of the government measures that were reported by the respondents included the signing of ACTS, capacity building and establishment of relevant institutions. Contrastingly, some respondents disagreed that, all actors are actively involved in cyber security. The figure below illustrates the distribution of respondent's opinions on how they rated their countries' cyber security effectiveness.

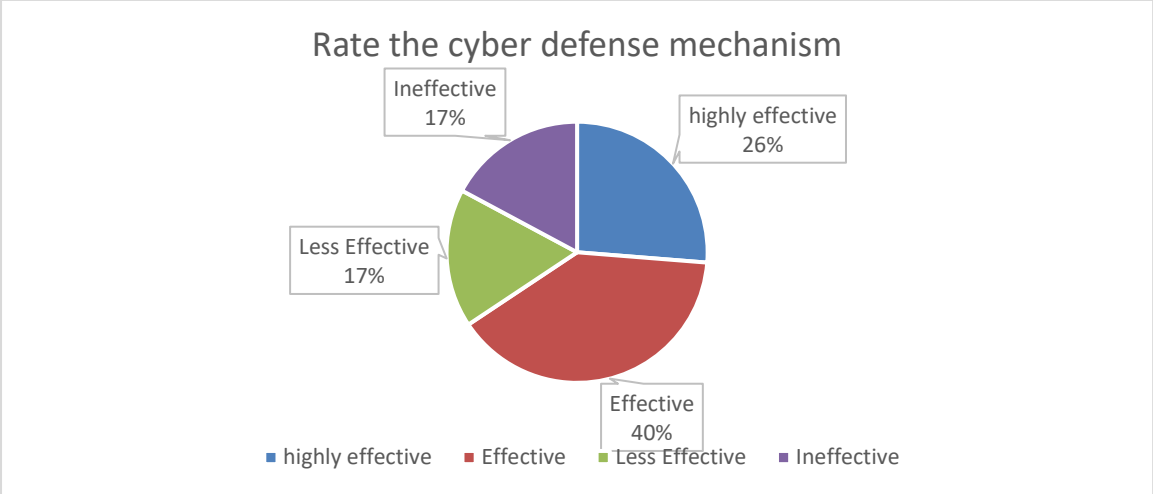

Figure 3.3: Rate of Cyber Defense Mechanisms in Kenya and Zimbabwe

Source: Field Data, 2020

It's worth noting that, there exist many differences and variances on the level of cyber integration into national security schemes between Zimbabwe and among different countries in the continent. It was noted that, developed countries had transformed cyber security initiatives into their national security structures as compared to developing countries. The difference on this transformation was attributed to differences in technological advancement and limited research available in developing countries. The researcher noted a greater disregard of cyber security

among developing countries.

3.7 Chapter Summary

Due to the increased cyber security threats the governments and stakeholders in both countries instituted measures and polices, aimed at combating these threats especially in the ICT sector. They adopted cyber defense mechanisms which include, establishment of technology which have digitalised registry and eco-system enhancing for better service delivery to the public. Zimbabwe drafted Bills relating to cyber security defences, which promoted the establishment of a legislative framework that would be used to administer the cyber space. Kenya also has defence mechanisms provided by various Acts which are regulated by the ministry of ICT and CAK. In addition, the countries also developed non-legal Cyber security mechanisms, such as public sensitisation campaigns, monitoring of exit and entry points, technological tools and innovations as well as mutual international cooperation. These legal and non-legal frameworks are aimed at curbing emerging cyber security threats and effective strategies of securing the cyber space.

CHAPTER FOUR

REGIONAL CYBER SECURITY DEFENCE STRATEGIESIN KENYA AND ZIMBABWE

4.0 Introduction

This chapter discusses the regional security responses instituted by the two countries to safeguard their systems against attacks targeting cyber space. The chapter will first, conceptualise the regional concepts of cyber security and consequently present findings on the responses which have been instituted to curb the spread of the cyber threats.

4.1 Regional Concepts of Cyber Security

Africa cyber security concept emerged in 1990s after the cold war period, when computer technology came to light. Initially, the term was thought to be related to networked computer, but later it was confirmed to be emerging from new cyber technologies.[133] Owing to the increasing threats, the (AU) in 2014 adopted the CCSP in Malabo, Guinea.[134] Although, the Convention focused on Cyber Security; the concept was not well understood except the explanation in the convention text. This is because cyberspace lies in the expansive global field. The Convention envisaged regulating the evolving technological domain which set forth the cyber rules on security as a critical step in establishing credible digital space for protecting the infrastructure.[135]

Arising from the convention, African states adopted different strategies to

[133]Singer, P., & Friedman, A. (2014). *Cyber security and Cyber war. What everyone needs to know*. New York: Oxford University Press.
[134] Abdulrauf, L., & Fombad, C. (2016). The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?. Tallinn, Estonia: CCDCOE
[135] Ibid p5

contain the threats peculiar to their environment.[136] Most nations such as Kenya, Uganda, Cameroon and Botswana started to enact cyber legislations and establish sub-regional collaboration instruments to combat cybercrime.[137] On the other hand, (ECOWAS) chose to adopt the various conventions aimed at safeguarding cyber security such as CML, CRC, the ECBCC and Directive to Fight Cybercrime.

Through the support of (ITU), the Kenyan Government in 2012 established the (KE-CIRT/CC). The unit was to assist in providing advice on technical supervision of cyber related crimes. It was delegated to guide and advice the Government on issues concerning national cyber security and coordinating all other agencies, both local and international on cyber incidence response mechanism. However, since its inception, the organisation has remained dormant, hence casting doubt on its role as a key national agency. This has also created doubt in its competence and therefore lost its relevance.

4.2 Challenges facing Cyber Security in African Region

All cyber security threats are similar in characteristics globally. However, the differences in the internet infrastructure connections especially in the African region distinguish it from the rest of the world.[138] The reason for the irregular connectivity is due to lack of technological capacity, which makes it susceptible to attacks especially in the public sectors, such as banking where the system network relies on machine run software which is obsolete and no longer supported by the manufacturer in some cases.

---

[136] Schell, B. Ho., & Clemens, M. (2004). Cybercrime: A Reference Handbook. Santa Barbara, California, United States : ABCCLIO

[137] Juma, V. (2010, August). Online Shopping Kenya Consumers out of KRA Reach. *Business Daily*, Available at https://www.businessdailyafrica.com/markets/Online-shopping-keeps-consumers-out-of-KRA-reach/539552-976992-2gr1vjz/index.html

[138] Gercke, M. (2006). *The Slow Wake of a global Approach against Cybercrime, Computer law Review International*. Oxford: Oxford University Press

The mobile industry also raises similar concerns of selling out outdated software's. In Addition, there is a lot of unsupported software and upgraded servers which exposes the whole ICT infrastructure to attacks. Another challenge is lack of reporting of cyber security incidents by some organisations when subjected to cyber-attacks.[139] This situation makes it difficult to establish the extent of cyber-attacks in Africa, which makes it hard to find solutions. Lack of capacity in information sharing, ineffective legislation and enforcement of law are key weaknesses in Africa internet infrastructure security, as indicated by Norton Cyber-Crime Report 2016.

4.3 The Trends of Threats Posed by Technology

The future of Africa science and technology is promising, despite the unprecedented advances of insecurity that are also growing fast.[140] The underground criminals are equally very innovative and are fast to adapt to any emerging technologies. Most of them have now developed their own encrypted communication networks, for example the Mexico Narcotic criminals and Al-Shabab with Improvised Explosives Devises (IED) in Somalia.

Cyber technology has made the world increasingly open, despite the huge benefits to the society. Criminals have also invested and deployed the same technologies in their field of operations.[141] For example, the Al-Shabab terrorists in Somalia have resorted to the use of remotely controlled IEDs, as weapon of choice against African Mission in Somalia (AMISOM) troops. The IEDs are homemade bomb technology, which have evolved over time and now come in many forms and

[139] Goel, S. (2011). Cyber warfare: Connecting the Dots in Cyber Intelligence. *Communications of the ACM*, 54(8), 132-140.
[140] Ben, B. (2011). Promoting Research and Development: The Government's Role. *Journal on Science and Technology,* 27(4), 23-145
[141]Greers, K. (2009). The Cyber Treat to National Critical Infrastructures; Beyond Theory. *Information Security Journal,* 18 (1),1-7

different levels of sophistications.[142] The IED innovations are initiated using cell phones that are remotely operated from a distance to avoid detection. Given the advancement in technology, the criminals have clearly shown their ability to seize the opportunity for their own advantage.

In addition the researcher sought to establish the most prevalent cyber threats in respective countries and established that, the most accounted cyber threats included; "external hackers, phishing scams, targeted distributed denial of service, computer viruses and worms, rogue spywares and software, defacement of websites, outdated systems and devices as well as cybersquatting". Asked if they had ever experienced any cyber threat,

"One of the respondents affirmed to a particular incident in the banking sector where customers' accounts where compromised and money lost. Another respondent stated; "in the DDO offices, the websites were breached and brought down". The respondent continued and stated that-"information was hacked from a computer and all data therein lost". Another incident involved phone swapping where money was lost".

4.4 Cyber Security Resilience Structures in Africa

Africa cybercrime and security discussions have tended to highlight hacking of information, terrorism or use of infectious malware amongst others.[143] It is evident that, very little attention has been given to these issues largely because of lack of knowledge and capacity to foresee threats from cyberspace.[144] The continent's cyber security resilience is intended to ensure that, in the occasion of a cyber-attack, there are measures to mitigate and in the event of failures, the system does not completely

[142]Bale, M. (2007). *Some Preliminary Observation on Jihadist Operation in Europe. In Workshop on Determining a Research Agenda for Disrupting IED Terror Campaigns: finding the Weak Links*. Irvine, California

[143]Farwell, J., & Rohozinski, R. (2011). Stuxnet and the future of Cyber War. *Global Politics and Strategy*.53(1), 23-40

[144] Lewis, A. J. (2002). Assessing the risks of Cyber Terrorism, Cyber War and Cyber Threats. *Journal of Centre for Strategic and International Studies*, 93(5), 22-27

collapse.[145]

Cyber resilience concept calls for a broad based approach, when dealing with cyber security, in order to develop strategies and measures which have been elusive to handle before. As observed the Western powers approach on the matter has been informed by their interest in Africa, especially on issues dealing with terrorism. This effort has been at the expense of in-depth cyber security programs for the entire continent hence remained in the Horn of Africa.[146]

It's on basis of this that AUCSPDP a body that handles continental cyber preparedness issues, has raised concerns on cyber security situation in the continent, with different security awareness levels. According to the Routine Activity theory, "cyber threats thrive when there is availability of suitable opportunities and the absence of adequate protection measures".[147] In translating this argument to cyber resilience measures in Africa, this shows that the efforts are not without challenges. The pursuit for well synchronised cyber security methods to address increasing cyber-attacks need to be treated with more political understanding than it is today. The UN has played a significant role in supporting the fight against cybercrimes in East Africa through its initiatives such as the larger anti-terrorist strategy. China has also invested in enhancing telecommunication networks in Africa especially in Ethiopia.

4.5 Regional approach to Cyber Security Threats

Africa development into the internet technology of doing business lacks institutional framework to address the threats which the internet poses. Whereas, a

[145]Ganuza, N., Hernandez, A., & Benavente, D. (2011). *An Introductory Study to Cyber Security in NEC" NATO Cooperative Cyber Defense Center of Excellence*. Tallinn, Estonia: CCDCoE
[146]Ploch, L. (2010). *Countering Terrorism in East Africa: The US Response. CRS Report for Congress*. Washington, D.C., United States: Congressional Research Service.
[147] Cohen, L., & Felson, M. (1997). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588-589.

few institutions have been established to fight cybercrimes, they are still weak to deal with the challenges presented by technology. The continent lacks clear policies on cyber security and the available laws cannot lead to any meaningful action.[148] The cases of cybercrime in Kenya is a pointer to the weaknesses of laws and policies on cybercrimes, largely due to absence of a government intervention to track and monitor online activities of suspects. This argument is true considering the way in which enforcement on perpetrators has been handled previously. The Kenya cyber security laws are weak and rarely provide effective remedies to suspects.[149]

This is a gap that is exacerbated by the weak political and institutions to enforce the law, and corruption which reflect lack of goodwill to fight the crimes. For example, it is noted that, some high-ranking officials in the government of Nigeria were involved in cybercrime of hacking bank accounts and stealing government information.[150] In many instances, the cybercrime laws have been noted to have gaps that allow hackers to operate without detection. The Kenya Communication (Amendment) Act 2009 prohibits hacking of an imposter website. Equally, the court system and law enforcement agencies lack adequate computer knowledge to be able to effectively combat cybercrimes.

However, it is encouraging to note that, with the enormous losses incurred through cybercrimes, Africa is waking up with cyber security initiatives. They are emerging security awareness measures through social learning programmes for academic writings.[151] Similarly, a framework is being developed to deal with cyber threats in the continent. Among these efforts is the establishment of cyber security

[148]Akogwu, S. (2012). *An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University*, Zaria (Unpublished B.Sc project).Zaria: Ahmadu Bello University, p.75.
[149]Kigen, P., et al (2014). *Kenya Cyber-Security Report 2014*. USIU: Nairobi, Kenya
[150]Kornakov, K. (2006). *Police forces in East Africa Will have a New Hi-tech lab*. Berlin, Germany: Springer
[151]Baumartner, F. R., & Jones, B.D. (1993). *Agenda and Instability in America Politics*. Chicago: University of Chicago Press.

export groups that are responsible for handling computer security events at both international and national levels. Tunisia, for example has established a first ACNSI Institute known as the (CERT TCC) which receives support from ITU (ITU, 2009). Others countries in Africa have established Africa Coordinating Centre for Africa CERTs in 2011.[152]

Further, Tunisia and South Africa have gone ahead to develop national cyber security framework and legislation for identification of electronic devices. These countries have strengthened their law enforcement skills and capacity to deal with cyber threats. Nigeria has equally followed and established a user awareness programme, as a strategy for national cyber security edge. The (EAC) states have also followed the example and made efforts to establish a cyber-science centre of excellence.[153]SADC formulated a law on "Computer Crime and Cybercrime" which was adopted in March 2012, to fight cyber threats. However, these laws have played an important role in fight against this menace. Further, the members have also made efforts in drafting bills and laws that will help to curb these threats. Likewise, Kenya had planned to establish a cybercrime laboratory referred to as forensic lab for use by national police, but this was not actualised due to corruption.[154]

In regard to the cyber defense mechanisms strategies which were adopted in their respective countries and generally in the African continent, with much emphasis on Kenya and in Zimbabwe as well as rating their effectiveness. The study established that, some of the defense strategies included; laws and legislations as well as policies, which provided an underlying framework for justification for all cyber defense

[152]Wanjiku, R. (2011). *Rising Cybercrime Pushes African Government to Take Action. Computer world Kenya*. Retrieved from http://news.idg.no/cw/art.cfm? id=6EF9B560-0DDE-E2CB-4D0981F70155CC24
[153]Muwanga, D. (2011). *East Africa Asked to Build Cyber Science School*. Retrieved from http://www.busiweek.com/11/opportunities/1997-east-africaasked-to-build-cyber-science-school
[154]Kornakov, K. (2006). *Police forces in East Africa Will have a New Hi-tech lab*. Berlin, Germany: Springer

initiatives, technology solutions and tools. Additionally, states have increased user awareness and knowledge transfer which provides the user and technology administrations, with knowledge on how to protect themselves in the cyber-space and system they administer. Some states have adopted computer emergency response teams, coupled with updating and installing software for backups. In majority of African states, cyber security threat response mechanisms entail use of anti-viruses and firewalls.[155] Other measures outlined included; regional and international cooperation, adopting cyber insurance, developing business continuity plans and invoking them as well as advancing the preparations to handle threats.

Further, majority of the respondents attested to the effectiveness of laws and policies which have helped to reduce the cyber threats and crimes. These legislative tools have provided institutionally based frameworks, for arrests and prosecution of cyber criminals in both countries. In both countries, governments have invested to a greater extend in security tools and solutions which safeguard national cyber space.

4.6 UN Regulations on Cyber Security and Cyberspace Operations

UN as the supranational body deliberated and made efforts to normalise the cyber space operations. The main arguments that were presented were those of the IL, the applicability of the law and ubiquity in handling the anticipated problems. The other attempt was to bring about open, protected, pacific and manageable cyber milieu.[156]

The UN Charter is clear and assertive that, states must uphold and respect the human rights conventions in their efforts to combat cyberspace crimes and safeguard human and national security. However, according to the UN Charter, states are

[155] Ibid
[156] Robert,G. (2012). *International Engagement on Cyber: Establishing Norms and Improving Security*. Washington, D.C., United States: Georgetown University Press

accountable to the transnational obligations arising from transnational and illegal actions that are attributed to them.[157] It is inevitably not permissible for states to let or make use of representations to conduct unlawful actions besides safeguarding their cyber spaces.

In relation to the above paragraphs and cognisant of the UN Charter, besides the maintenance of international peace and stability, states are empowered through the UN Charter provisions to protect themselves by coming up with necessary mechanisms for cooperation and use techniques, to surge stability and security in their cyberspaces. The states have an obligation of preventing cyber space operations that are inconsistent with laid down procedures and rules of operating peacefully in coexistence with other states.[158]

4.7 Cyber Security Threats Response Institutions in Kenya

In Kenya, cyber security is regulated by the (NCSC). The main state actors in investigating cybercrimes include; CSIRT-Kenya, and the CSIRT under the auspices of the MICT.[159] There are also available mechanisms, procedures and policies for or safeguarding these threats and response to cyber security incidents in Kenya.

The main functions of the institutes are to identify, defend and salvage in combating cybercrimes and threats. Threats are analysed and categorised in accordance to the laid down classifications adopted in Kenya.[160] The institutions work in tandem with the security operations centre for the government to produce new policies protecting the cyber environment, threat evaluation and application of

[157]Buzan B., & Waever, O. (2003). *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press, p 27-30.
[158]Ibid, p 11.
[159]CAK. (2019). A *Collaborative Approach to National Cyber security Resilience*. A Collaborative Approach to National Cyber security Resilience. Nairobi, Kenya
[160]Ibid

strengthening the existing cyber defence mechanisms. Kenya is progressing with the implementation of the (NCSMS) as implored by President of Kenya, Uhuru Kenyatta in June 2014. The cyber security and other related pieces of legislation majority of which are being in later stages of formulation are yet to be promulgated as the legislative laws.

The national cyber security awareness campaigns are spearheaded by the MICT as emphasised in the NCSMS. The NCSMS programmes are conducted jointly with the Kenya Communications Authority. In addition, the academia continues to run cyber security related degree programmes in the tertiary education, as well as the institutions promulgated by government, to spearhead the cyber security awareness concerns in the government structures.

There is a multi-faceted approach, as the Government of Kenya works together with the stakeholders in the state. It's worth noting that, different stakeholders and actors have collaborated to provide and enhance defence mechanisms which will assist in combating cyber threats and crimes. Furthermore, Kenya continues to cooperate with other major players like Google, Sophos and others in enhancing cyber security. The main theme is confidence building, procedures and international collaboration. This is enhanced in order to share information; preeminent rehearsals for cyber security in the UNGCS.

States pursue transnational collaboration on the precarious infrastructures weaknesses. The procedures or the fountains are that the state's acts and strategies are aimed at safeguarding its networks. It is imperative to share periodical resources considered to be suitable amongst states' legal structures and institutions. The established cooperation will enhance the structures and progressions, sessions on

defences and cyber security threats on the critical infrastructure.[161] The espousals of deliberate domestic provisions of the laws and institutions for assisting information exchange will enable any state to respond to the cyber security threats.

4.8 Implementation of Cyber Defence Mechanisms Regionally

Majority of the respondents agreed that, their countries have started implementing cyber security defense mechanisms to cushion the countries against threats imposed by cyber criminals. The researcher asked the respondents to rate the level of implementation of cyber defence mechanisms regionally and the ratings were tabulated as shown below;

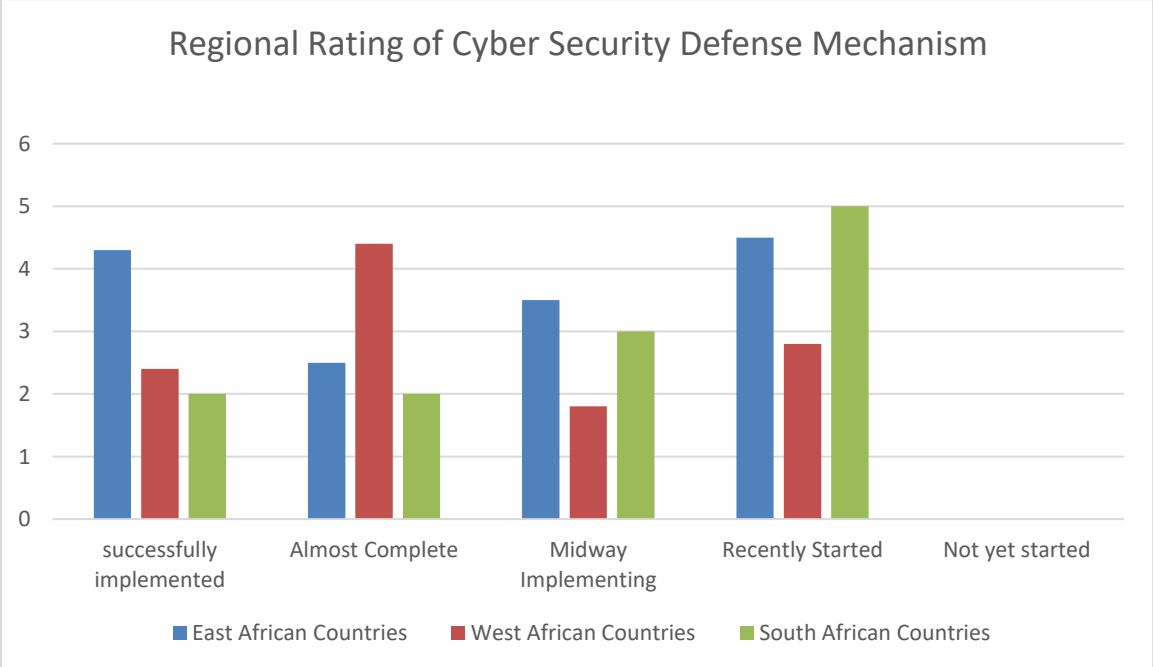

Figure 4.1: Regional rating of cyber defense mechanisms

Source: Field Data, 2020

Most of the respondents asserted that most countries in the respective African

[161] Kigen, P. (2015). *Kenya Cyber Security Report 2015: Achieving Enterprise Cyber Resilience through Situational Awareness.*Berlin, Germany: Research Gate

regions had started implementing cyber security defense mechanisms, because the cyber security in most of these countries was a new concept that was being adopted by majority of the people through use of technology. The respondents posited that, majority of the sectors in their respective countries' economies, had started implementing cyber defence mechanism in sectors, such as the finance sectors, telecommunication, transport, health, education and transport.

4.9 Non-Legislative Cyber Security Schemes in Kenya and Zimbabwe

The researcher sought to establish other cyber security threats mechanism other than "legal and institutional frameworks" that have been used in the management of cyber-attacks in both Kenya and Zimbabwe. The figure below shows some of the non-legislative measures that have been adopted and integrated into national cyber security schemes in both Kenya and Zimbabwe.

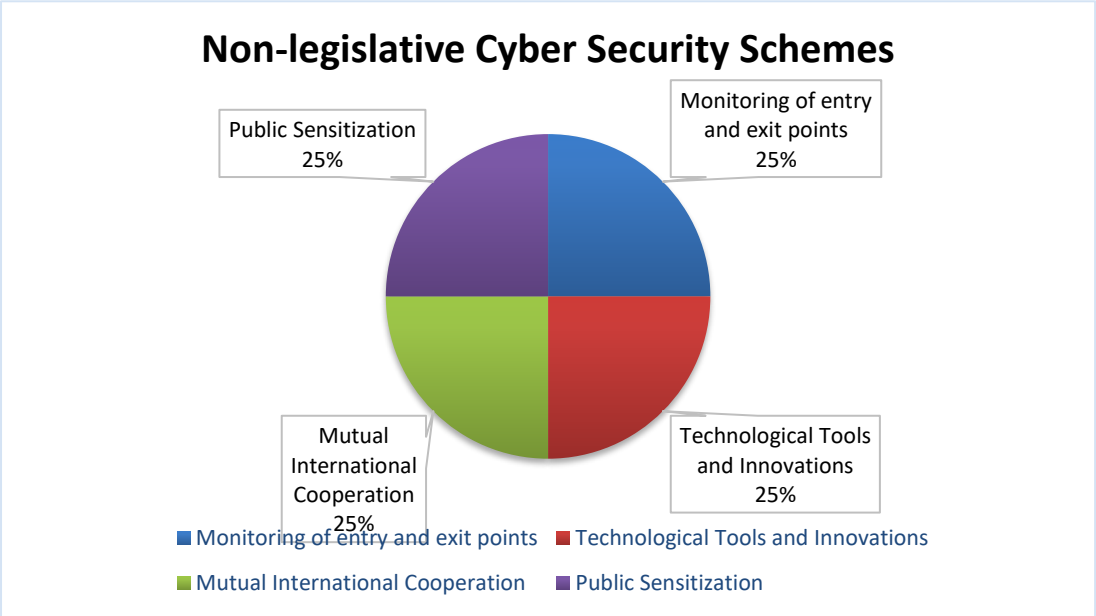

Figure 4.2: Non-Legislative Cyber Security Schemes in Kenya and Zimbabwe

Source: Field Data, 2020

The study endeared to assess the impact that, the cyber security mechanisms had on respective country's cyber security structures and determined that; utilisation of advanced software, training and awareness creation had led to improvement in cyber threat detection and protection in both countries as well as the rising consciousness of the threats imposed by cyber criminals among the consumers. Additionally, these security mechanisms have provided benchmark standards for improving proficiency of people tasked with cyber security. In determining the effectiveness of the cyber security schemes, the researcher, asked the respondents to rate the effectiveness of these measures. Affirmatively, majority of the respondents noted that, apart from the legislative measures being effective in curbing cyber security threats, there exist other measures (non-legal measures) which rated highly effective in improving cyber security. The table below shows respondents perceptions on the rate of effectiveness of non-legislative cyber security measures adopted by the two countries.

Table 4.1: Effectiveness of Non-Legislative Cyber Security Measures in Kenya and Zimbabwe

Non-legislative Cyber Security Measures adopted in Kenya and Zimbabwe	**Level of Effectiveness**	**Number of Respondents**	**Per cent (%)**
✓ Awareness ✓ International Cooperation ✓ Technological Advancement ✓ Border Control	Highly effective	18	39
	Effective	10	22
	Less Effective	6	13
	Ineffective	8	17
	Highly Ineffective	4	9
	Total	**46**	**100**

Source: Field Data, 2020

Majority of the respondents (39%) agreed that cyber security awareness measures have been effective by creating awareness of the threats in existence and developing countermeasures which have been rated as highly effective. The effectiveness of the countermeasures have focused mainly on sharing of information, technical adjustments and location visits, cross-border screening, arrest and prosecution of offenders, creation of awareness in supporting and implementing of legal frameworks. With those who cited ineffectiveness in the cyber security apparatus, they justified the same by attributing it to, lack of testing to prove ineffectiveness or effectiveness, as well as opposition from civil society groups which cite confidentiality and privacy reasons as major hindrances to cyber security mechanism as they related to human rights.

It is generalised that both legislative and non-legislative cyber security interventions, have been effective in curbing the emergent cyber threats, as evidenced empirically by a majority tally of most of the respondents. They agreed in their effectiveness in the criminal handling of the cases attributed to cyber security, as well as avoiding delays and hurdles, put across by those who oppose cyber security. According to Nyireda-jere & Biru, there is the African Union Convention on Cyber-security and the Personal Data Protection 2014, which have been domesticated both in Kenya and in Zimbabwe.[162] These legislations seek to harmonise African cyber legislations.

There are other security related threats which are prioritised higher in both Kenya and Zimbabwe than cyber security threats. These threats are central to people's livelihoods and their imperative subjects. The respective countries will also render subsequent attention to the cyber security threats which are deemed secondary or not

[162] Nyirenda-Jere, T., & Biru, T. (2015*). Internet development and Internet governance in Africa*. Geneva: Internet Society

of much priority. The researcher sought to establish if these competing interests jeopardise cyber security implementation mechanisms and efforts in the respective countries. Majority of the respondents (43%) agreed with the notion of competing interest as compromising the implementation of cyber security in both countries. This is attested to by the number of cyber security threats which have hit each country. For instance; Zimbabwe is considered vulnerable to terrorism attacks coordinated through the cyber space, due to its unpreparedness in terms of these threats. This is evidenced by a case where government delicate information was shared through hacking of its websites.[163]

4.10 Chapter Summary

It's evident that a number of regional and continental-wide legislative frameworks have been adopted by the two countries and domesticated into national laws. Regionally, the establishment of (HIPSSA) constitutes a model law which (SADC) states, refers to in drafting their cyber laws. However, both legislative and non-legislative cyber security interventions have been effective in curbing the emergent cyber threats. This has led to improvement in cyber threat detection and protection in both countries, as well rising consciousness of the threats imposed by cyber criminals among the consumers. Additionally, these security mechanisms have provided benchmark standards for improving proficiency of people tasked with cyber security.

[163] Ibid. p.5

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary of findings established by this research study as well and offers a comprehensive conclusion derived from the comprehension of emerging cyber security threats utilising a comparative study of Kenya and Zimbabwe. Finally, the chapter shall provide tailor-made policy recommendations suitable for both Countries.

5.2 Summary of Findings

In regard to the first objective, the study has established a number of legislative tools available in both countries, which facilitate attainment of cyber security. Whereas, Kenya has enacted a number of cyber security related legislations, Zimbabwe lacks a comprehensive "Cyber security framework" anchored in law, which could inform national strategy on cyber security. Kenya has domesticated the COMESA and enacted the KCSCB to form part of Kenyan Cyber legislation and law. Primary data has corroborated the available data with assertion that, legislation and regulation have formed the core basis through which respective countries have instituted cyber security strategies, with majority of respondents outlining some of the laws, protocols and conventions adopted by their countries.

The need to develop national Cyber security legislation is informed by the realisation that, cybercrimes led to negative impacts on the country's economy and development as well as threatening both national and human security. These devastating impacts have been experienced by countries worldwide including

Zimbabwe and in Kenya.

In regard to the second objective, this research has discovered that, in response to the emerging growth of cyber threats in both countries, respective government key security stakeholders have made efforts to curb these menaces especially in the ICT sector, through enactment of various cyber defence mechanisms.

The study established that Zimbabwe has enacted various Bills relating to cyber security defenses, which promoted the establishment of a legislative framework that would be used to administer the cyber space. Also the ZRP, National Intelligence Services and the ZDF are part of the institution enforcing the governance of the cyber security. These legislative defences have been supplemented by other non-legal cyber security mechanisms, which entail public sensitisation campaigns, monitoring of exit and entry points, technological tools and innovations as well as mutual international cooperation.

Kenya on the other hand has adopted cyber defence mechanisms aimed at combating cybercrimes. These mechanisms are under mandates of ministry of ICT and the (CAK). Notably, this research established that, in policies regarding to cyber space are formulated by the ICT through the NCSMP, while in Zimbabwe the Cybercrime and Cyber Security Bill (2017) presents the country's legislative framework for cyber security, although it has been accused severally for violation of human rights by civil societies. Primary data confirms the existence of various legal means and generally the various instruments and tools for curbing the emerging cyber security threats as effective strategies of securing the cyber space.

Lastly, in line with the third objective, the study analysed several regional cyber security architecture master plans and continent-wide legal instruments concerned with cyber security. The study has established a number of regional and

continental-wide legislative frameworks, which have been adopted by the two countries and domesticated into national laws.

In Kenya, regional cyber security defence strategies include the COMESA-CSCR-EA which form part of the regional cyber security defense strategy domesticated into Kenyan laws. Other binding conventions and protocols which have been ratified by Kenyan state include; ITU, OECD, APEC TEL and FIRST which ensure national laws are developed within international cooperation principles of Cyber security. Primary data has attested to the effectiveness of regional cyber security strategies, in improving state capacities to handle emerging cyber threats.

5.3 Conclusion

The study finds that, national cyber security is a real and growing threat to the national security interest, posed to both Kenya and Zimbabwe as they seek to invest and enhance their ICT capabilities and infrastructures. The threats of Cyber-attacks have grown in scale and in sophistication over the last ten years, with emerging threats that are detrimental to the security of the state and regional stability. Among the major cyber threats experienced in both Kenya and Zimbabwe include; malware, hacking, phishing, viruses and spams.

These cyber threats are common in both countries and this study has determined that they are perpetrated by criminal groups and other malicious actors with support from foreign countries. To cushion their states and nationals from these threats, both Kenya and Zimbabwe have adopted both legislative and non-legislative strategies as well as defence mechanisms, discussed earlier to curb the emerging threats with Kenya fostering a great milestone in measures aimed at regulating the domain. This confirms second and third hypotheses on the availability of legal

frameworks and defense mechanism strategies adopted by both countries to curb cyber threats. Comparatively, Kenya leads the region other than in EAC and SADC countries in her cyber security strategies which can be benchmarked by other countries for effective cyber space security.

However, Zimbabwe though establishing Bills relating to cyber security defences lacks a comprehensive "cyber security framework" anchored in law, which could inform national strategy on cyber security. This confirms the first hypotheses that, there are sufficient legal frameworks and institutions in Kenya and Zimbabwe to respond to cyber security threats. Therefore, there is need for the governments of both countries to adopt and formulate more robust policies, and frameworks that will help in the fight against cybercrimes which are detrimental to both human and national security.

5.4 Recommendations

This research study has formulated some tailor-made policy recommendations suitable for developing countries, as they formulate legislations, protocols and strategies for securing the cyber space. Good cyber security policies and practices should put people and their rights, at the center and seek to strengthen and protect human rights rather than curtail them. In regard to the first objective, governments in both countries (Kenya and Zimbabwe) should;

- Establish a cyber-security "framework" rather than one law in isolation. Cyber security is made up of different, complementary initiatives and approaches. Legislation may be just one of these elements. Many elements of cyber security rely on non-legal mechanisms, such as minimum standards of security, investment in security research, security audits of key industries

and public bodies. Government policy in this area can make a real difference in raising standards of security.

- Establish comprehensive legal frameworks around "cyber enabled crimes". This refers to established crimes committees in a new way using technology, such as fraud or distribution of child abuse images. The standard inclusion of these kinds of crimes in cybercrime laws aids cross border co-operation in solving them. However, these crimes should not only appear in a cybercrime law. For example, distributing child abuse images is a crime whether using a computer or not. Therefore, it should be supported by a comprehensive child protection legal framework where the crime can be defined more precisely, and importantly, contextualised in its broader context.
- Adopt and implement a comprehensive data protection law. Cyber security frameworks must include data protection laws which safeguard against the exploitation of personal data collected by companies and public bodies. Without legal obligations to protect personal data from abuse by companies and public bodies as well, people will be left vulnerable to situations in which their data is excessively collected, poorly secured and ultimately at risk of being stolen.

In reference to the second objective, the governments in both countries (Kenya and Zimbabwe) should;

- Establish a clear, accessible and comprehensive cyber defence mechanism which should be debated with public consultation and stakeholder involvement. The public and businesses must have an idea of the real threats they face and contribute to the discussion on how they can protect themselves.

Lastly, in line with the third objective; the governments in both countries (Kenya and Zimbabwe) should;

- Establish incident response teams. These teams of experts are the frontline for when a security incident happens, and mostly deal with compromised devices or services that are enabling cyber-attacks. Ideally, they would want to be independent of government departments they should cooperate and strongly corroborate the government efforts.
- Undertake a proper threat assessment. A threat assessment considers possible weaknesses, such as outdated infrastructure, that make the country more vulnerable to attack, and help in decision-making and prioritisation.
- Develop a strong and Rights-respecting cybercrime approach. A cybercrime law should not be an excuse to include an extended list of crimes that ultimately violates international human rights law. Examples of crimes that are not cyber-crime include criticising the government on social media and using encrypted messaging services as and when not authorized by the state.

.

REFERENCES

Abdulrauf, L., & Fombad, C. (2016). *The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?*.Tallinn, Estonia: CCDCOE

Acemoglu, D., & Robinson, J. (2012). *Why nations fail: The origins of power, prosperity and poverty*. New York: Crown Publishers

Akogwu, S. (2012). *An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University*, Zaria (Unpublished B.Sc project).Zaria: Ahmadu Bello University, p.75.

Alan, C. *(2003). Security and South East Asia: Domestic, Regional and Global Issues.* Colorado: Lynne Rienne Publishers Inc.

Alanezi, F.et al. (2014). *Combatting Online Fraud in Saudi Arabia Using General Deterrence Theory (GDT).*London: Brunel University

Amos, A. (2009). *American Security*, 6th Ed., Baltimore: The Johns Hopkins University Press

Andrews, M. (2013). *The limits of institutional reform in development*. New York: Cambridge University Press.

Armiger, B. (2019). Ethics in Nursing Research: Profile, Principles, Perspective. *Nursing Research*, 26 (5), 330-333

Austin, G. (2012). The Cyber security: Shared Risks, Shared Responsibilities. *A Journal of Law and Policy for theInformation* Society, 8 (2), 81-103

Baezner, M. (2018). *Cyber- security in Sino-American Relations*. ETH Zurich: Center for Security Studies

Bale, M. (2007). *Some Preliminary Observation on Jihadist Operation in Europe. In Workshop on Determining a Research Agenda for Disrupting IED Terror Campaigns: finding the Weak Links*. Irvine, California

Barry, B., &Little,R.(2000). *International Systems in World History: Remaking the Study of International Relations,* 1st Ed. Oxford: Oxford University Press

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

Ben, B. (2011). Promoting Research and Development: The Government's Role. *Journal on Science and Technology,* 27(4), 23-145

Boulanin. V. (2017). *The development and discussion on LAWS Chapter*. Oxford: Oxford University Press

Bourne, M. (2004). *Understanding Security.* London: Palgrave, Macmillan

Brencil, K. (2018). *Kenya Cyber Security Report 2018*. Nairobi: SERIANU Publication

Bryman, A. (2012). *Social Research Methods,* 4th Ed. Oxford: Oxford University Press. pp. 186-187.

Buse, C. (2009). When you retire, does everything become Leisure? Information and Communication Technology Use and the Work/Leisure Boundary in Retirement'. *New Media and Society*, 11(7), 1143-61.

Buzan B. and Waever O, *Regions and Powers: The Structure of International Security,* Cambridge, Cambridge University Press, 2003, p 27-30.

Buzan, B & Little, R. (2000). *International Systems in World History: remaking the study of International Relations.*New York: Oxford University Press.

Buzan, B,. & Waever, O. (2003). *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press.

Buzan, B. (2016). *People, States and Fear: an agenda for international security studies in the post-cold war era*. Colchester: ECPR Press.

Buzan, B., & Little, R. (2000). *International Systems in World History: remaking the study of International Relations.* New York: Oxford University Press

CAK. (2019). A *Collaborative Approach to National Cyber security Resilience*. A Collaborative Approach to National Cyber security Resilience. Nairobi, Kenya

Cavelty, M. D. (2007). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (1st ed). Boulder: Lynne Rienner

Cohen, L., & Felson, M. (1997). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588-589.

Creswell, J W. (2014). *Research Design*, 4th Ed. Lincoln: University of Nebraska

CyberCity,E. (2018).*Media Statement SADC Capacity Building Workshop on Cyber Security and SADC Regional Cyber Drill.* Mauritius

David, E. (2005). *The Mosaic Theory, National Security, and the Freedom of Information Act*. *The Yale Law Journal*, 115 (3)

Desmond, B., & Gary, W. (2013). Security Challenges. *Journal of Regional Security*, 9(2)

Dighton, F. (2015). , *Defining a Framework for Decision Making in Cyberspace: Strengthening Cyber-security Series.* Pennsylvania: Indiana University Press

Douglass, N. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press

Douwe, K. (2011). *The definition of cyber security*. Oxford: University of Oxford

Dover, R. (2009). Towards a Common EU Immigration Policy: a Securitization Too Far.*Journal of European Integration,* 30(1), 113-130

Dunn, T.A. (2008). *Imaging second messenger dynamics in developing neural circuits.*Rockville Pike: National Center for Biotechnology Information

Farwell, J., & Rohozinski, R. (2011). Stuxnet and the future of Cyber War. *Global Politics and Strategy*.53 (1), 23-40

Finklea, M. et al. (2015). *Cyber Intrusion into U.S. Office of Personnel Management: Congressional Report*. Library of Congress. Washington DC,: Congressional Research Service

Gagliardone,I., & Sambuli, N. (2015). *Cyber Security and Cyber Resilience in East Africa*. Waterloo, Ontario, Canada: Centre for International Governance Innovation and Chatham House

Ganuza, N., Hernandez, A., & Benavente, D. (2011). *An Introductory Study to Cyber Security in NEC" NATO Cooperative Cyber Defense Center of Excellence*. Tallinn, Estonia: CCDCoE

Gercke, M. (2006). *The Slow Wake of a global Approach against Cybercrime, Computer law Review International*. Oxford: Oxford University Press

Goel, S. (2011). Cyber warfare: Connecting the Dots in Cyber Intelligence. *Communications of the ACM*, 54(8), 132-140.

Gok. (2010). *the Constitution of Kenya 2010*. Nairobi: Government Press

GoK. (2014). *Kenya Broadcasting Corporation Act*. Nairobi: Government Press

Gok. (2018). *the Kenya Gazette Supplement Act. Nairobi*: Government Press

Gok. (2019). *the Kenya Information and Communication Act*. Nairobi: Government Press

GoZ. (2000). *the Postal and telecommunication Act of Zimbabwe, chapter 12.* Harare: Government Press

GoZ. (2006). *the Criminal Code (Codification and Reforms Act), Chapter 9:23*. Harare: Government Press

GoZ. (2013). *Access to Information and Protection of Privacy Act, Chapter 10:27*. Harare: Government Press

GoZ. (2013). *the Constitution of Zimbabwe Act no 20*. Harare: Government Press

GoZ. (2013). *the ZDF Act,Chapter 11:02*. Harare: Government Press

GoZ. (2016*). the Statutory Instrument the Post and Telecommunications (Consumer Protection) Regulations*. Harare: Government Press

Greers, K. (2009). The Cyber Treat to National Critical Infrastructures; Beyond Theory. *Information Security Journal,* 18 (1), 1-7

Gustav, L. (2012). *Meeting the Cyber Security Challenge*. GCSP Geneva Papers- Research Series no. 7. Geneva, Switzerland

Haddon, L., & Silverstone, R. (1992). *Information and Communication Technologies in the Home: The Case of Teleworking,* Working Paper 17. Falmer, Brighton BN1 9RH, United Kingdom: University of Sussex

Hansen,.L., & Nissenbaum, H. (2009). *Digital Disaster, Cyber Security, and the Copenhagen School.* New York: New York University

HDR. (1994). *Human Development Report*. Oxford: Oxford University Press

Hodgson, G.M. (2006). What Are Institutions?. *Journal of Economic Issues,* 40(1), 1- 25

ITU Report. (2018). Measuring *the Information Society Report.* Geneva, Switzerland.

James, L., & Katrina, T. (2011). *Cyber-security and Cyber-warfare, Preliminary Assessment of National Doctrine and Organization.* Washington, D.C.: Center for Strategic and International Studies

Juma, V. (2010, August). Online Shopping Kenya Consumers out of KRA Reach. *Business Daily*, Available at https://www.businessdailyafrica.com/markets/Online-shopping-keeps-consumers-out-of-KRA-reach/539552-976992-2gr1vjz/index.html

Kabanda,G. (2020). *A Cyber security Culture Framework and Its Impact on Zimbabwean Organizations*. Honolulu, Hawaii: Atlantic International University

Karuppannan, J. (2008). *Cyber criminology & cyber forensics Space Transition Theory of Cyber Crimes.* New Delhi, India:MHRD

Kelly, J. (2015).Strategic perspectives on cyber-security management and public policies. *European Cyber-security Journal*, 1(1), 26-72

Kigen, P. (2015). *Kenya Cyber Security Report 2015: Achieving Enterprise Cyber Resilience through Situational Awareness.* Berlin, Germany: Research Gate

Kigen, P., et al (2014). *Kenya Cyber-Security Report 2014*. USIU: Nairobi, Kenya

Kornakov, K. (2006). *Police forces in East Africa Will have a New Hi-tech lab*. Berlin, Germany: Springer

Kothari, R C, (2003). *Research Methodologies*, 3rd Edition. New Delhi: WishwaPrakashan

Landler, M., & Markoff, J. (2007). *Digital Fears Emerge After Data Siege in Estonia.* New York:The New York Times Company

Lars, B., Steffen, J., & Finn, S. (2007). *The Security-Development Nexus Expressions of Sovereignty and Securitization in Southern Africa*. Cape Town, South Africa

Lewis, A. J. (2002). Assessing the risks of Cyber Terrorism, Cyber War and Cyber Threats. *Journal of Centre for Strategic and International Studies*, 93(5), 22- 27

Marianna, M. (2011). What are the Major Ethical Issues in Conducting Research? Is there a Conflict between the Research Ethics and the Nature of Nursing?. *Department of Nursing Health Science Journal*, 5(2), 3-15

Maslennikov, D. (2012). *Kaspersky Security Bulletin 2012.The overall statistics for 2012. Available at* https://securelist.com/kaspersky-security-bulletin-2012-the-overall-statistics-for-2012/36703/

McGrath, A., & Lianos, H. (2017). *Can the General Theory of Crime and General Strain Theory Explain Cyberbullying Perpetration?*. Panoram: Charles Sturt University Press

Mugenda, A.G. (2011). *Social Science Research, Theory and Principles.*Nairobi: Applied Research & Training Services.

Muwanga, D. (2011). *East Africa Asked to Build Cyber Science School*. Retrieved from http://www.busiweek.com/11/opportunities/1997-east-africaasked-to-build-cyber-science-school

NirKshetr. (2019). Cybercrime and Cyber security in Africa. *Journal of Global Information Technology*, 6-7

Nyirenda-Jere, T., & Biru, T. (2015*). Internet development and Internet governance in Africa*. Geneva: Internet Society

Perloth.N, (2012). *In Cyber-attack on Saudi Firm, U.S. Sees Iran Firing Back. Available at* https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Ploch, L. (2010). *Countering Terrorism in East Africa: The US Response. CRS Report for Congress*. Washington, D.C., United States: Congressional Research Service.

POTRAZ. (2018). Post *and Telecommunications Regulatory Authority in Zimbabwe Report*. Accessed on https://www.itu.int/en/ITUD/Conferences/GSR/2019/Documents/ZimbabweContribution-GSR-19.pdf

Rain, O. (2019). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective Cooperative Cyber Defence Centre of Excellence*. Tallinn, Estonia: Academic Publishing Limited

Ritchie, J., & Lewis, J. (2004). *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. New Dehli: Sage Publishers

Robert, G. (2012). *International Engagement on Cyber: Establishing Norms and Improving Security*. Washington, D.C., United States: Georgetown University Press

Schell, B. Ho., & Clemens, M. (2004). *Cybercrime: AReference Handbook. Santa Barbara, California, United States*: ABCCLIO

Sergei, K., Sergei, K., & Igor, D. (2007). *Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law*. Moscow,Russia: ICTS and international security

Sico van, M. (2018). *State-level responses to massive Policy Brief cyber-attacks: a policy toolbox.* Amsterdam: Clingendael – the Netherlands Institute of International elations.

Singer, P., & Friedman, A. (2014). *Cyber security and Cyber war. What everyone needs to know*. New York: Oxford University Press.

Snow, D.M. (2004). *National Security for a New Era: Globalization and Geopolitics*. New York: Pearson Education

Sofaer.A.D. Clark, D., &Diffie,W.(2010). *Cyberspace and International Relations: Theory, Prospects and Challenges.* Springer;Berlin, Germany

Souhila, A. (2016). *ITU-ATU Workshop on Cyber-security Strategy in African Countries Khartoum, Sudan.* Addis Ababa: AU Commission

Stefan, F. (2005).*Cyberspace Security: A definition and a description of remaining problems*. Vienna: University Vienna - Institute of Government & European Studies

Stefik,M. (1997). *Internet Dreams: Archetypes, Myths and Metaphor*. Cambridge, Massachusetts: The MIT Press

Straub, W., & Welke, R. J. (1998). *Coping with systems risk: security planning models for management decision making*. Hong Kong: Management Information Systems, p 441-469.

Veritas. (2019). *Zimbabwe National Policy for ICT 2016-2020.* Harare, Zimbabwe

Walls, A., Perkins, E., & Weiss, J. (2013). *Definition: of Cyber security.* Stamford, Connecticut, United States:Gartner Inc

Wanjiku, R. (2011). *Rising Cybercrime Pushes African Government to Take Action. Computer world Kenya*. Retrieved from http://news.idg.no/cw/art.cfm?id=6EF9B560-0DDE-E2CB-4D0981F70155CC24

Wei, S. et al. (2010). *Superficial simplicity of the 2010 El Mayor–Cucapah earthquake of Baja California in Mexico.* Pasadena, California: California Institute of Technology

WTO. (2019). *Telecommunications Services*. Geneva, Switzerland: WTO

APPENDIX I: Data Collection Questionnaire

My name is Colonel F Taruvinga, a senior officer in the Zimbabwe Defence Force (ZDF) and also a student pursuing a Master's Degree in International Relations from the University of Nairobi, in collaboration with the National Defence College in Kenya. Part of my program requires that I conduct a study based on security and international relations from the area of my choice and interest. My research topic is on "Emerging cyber security threats: A comparative study of Kenya and Zimbabwe".

The purpose of this research is to investigate the extent to which the two countries can respond to the cyber security threats as defined in the ITU, AU the EAC and SADC implementation plans. This is both a human security concern and national security area. The security threats to the national security basing on the whether the concepts of security in these two state have incorporated human security. The study will further evaluate the strategies that have been put in place by government to mitigate against the threats.

The questionnaires are designed for this research only. You are kindly requested to fill in the questionnaire which will be used in the study. I assure you that the information gathered will be used for the purpose of this research only and will be treated with strict confidentiality. Thank you in advance for your cooperation.

Part A: General Information

Tick the appropriate answer to your level best

1. Gender

Male [ ] Male [ ]

2. Age

15-35 [ ] 36-50 [ ] 51-65 [ ] above 65 [ ]

3. Level of education

Primary [ ] Secondary [ ] University [ ] None [ ]

4. Marital status

Single [ ] Married [ ] Separated [ ] Divorced [ ]

5. Occupation

Self-employed [ ] Casual [ ] Formal employed [ ] Unemployed [ ]

Please specify type of employment and nature of your work?

…….

6. Which country are you from?

…….

Part 2: Legal Frameworks and Institutions in the Country

This section entails legal frameworks and institutions in either in Kenya and Zimbabwe.

1. What do you understand by the concept cyber security?

……
……
……
……
……

2. Which are the legal frameworks, laws and instructions in your country?

.....
.....
.....
..... ……

3. Briefly explain the effectiveness of the frameworks, laws and instructions listed above in managing cyber security.

……

……

……

……

4. Explain how you understand stand by cyber security being part of national security.

……

……

……

……

Part 3: Cyber Defence Mechanisms available in the country

1. Kindly mention the cyber defense mechanisms that have been adopted in your country to safeguard the current cyber threats?

……

……

……

……

2. Rate you're the effectiveness of the above mentioned cyber defense mechanisms in combating cyber threats in your country in a scale of 1 = strongly agree, 2 = Agree, 3 = Un-decided, 4 = Disagree and 5 = strongly disagree respectively

……

……

……

……

3. In your opinion are there any non-legal Cyber security mechanisms adopted in your country to protect the cyber security space?

……

……

……
……

4. Have the cyber defense mechanisms that have been adopted in your country to safeguard the current cyber threats being fully implemented?

……
……
……
……

Part 4: Regional Cyber Defence Strategies adopted in your Country

1. Are there cyber security threats defence mechanisms in the African region?

Yes ( ) No ( )

If you agree, kindly mention them?

……
……
……
……

2. Please outline at least five (05) of the most prevalent cyber threats in your country?

……
……
……
……

3. Do you agree that countries or states in the African region have started implementing cyber defence mechanisms?

Yes ( ) No ( )

a. If you agree list at least five STATES and give your rating in a scale of;

5=successfully implemented, 4=almost complete, 3=midway implementing, 2=recently started, 1=not yet started.

……
……
……
……
……

b. Explain your answer:

……
……
……
……
……

4. Do you agree that some sectors of the economy have implemented the cyber defence mechanisms in your country?

Yes ( ) No ( )

If yes name the sectors?

……
……
……
……

5. Kindly rate the sectors mentioned above in a scale of 1=best, 2= better, 3= good, 4=still need attention, 5=needs total attention.

……
……
……
……
……

6. Which are the cyber defence strategies put in place in the African region? Kindly pay particular attention to either Kenya or Zimbabwe or both of them. State and rate them starting from the one perceived as the most effective:

……

……

……

……

……

7. Please give an outline of the most cyber security threats response mechanisms in the African region and rate their effectiveness?

……

……

……

……

……

8. Do you think Kenya and Zimbabwe have peculiar cyber threats?

Briefly explain your answer?

……..……

……

……

……

……

9. In your opinion are there any achievements in the fight against cyber threats?

Briefly explain your answer?

……

……

……

……

10. Have you ever experienced any first-hand form of cyber threats in your line of duty?

Yes ( ) No ( )

If yes please explain

……

……

……

……

11. Cyber security integration into national security schemes in the African region, often have many differences compared to those of developed countries? Do you agree?

Yes ( ) no ( )

If yes kindly give a small assertive narration.

……

……

……

……

12. Describe other cyber security threats mechanism other than legal and institutional frameworks that have been used in the management cyber-attacks in Kenya or Zimbabwe or both of them.

……

……

……

……

13. Have your country collaborated with other countries in the African region to fight cyber security threats?

Yes ( ) No ( )

Has it been successful?

……

……

……

……

14. Are there any strategies that have not been effective in addressing the increasing cyber security threats in Kenya and Zimbabwe?

Yes ( ) No ( )

Briefly explain your answer.

……
……
……
……

15. What is your opinion on the effectiveness of unilateral intervention methods in cyber security threats management?

……
……
……
……

16(a) Do you think there are competing interests among the ICTs in Kenya and Zimbabwe?

Yes ( ) No ( )

b. If your answer is yes, do you think such competing interests will jeopardize cyber defences implementation efforts in the country? Explain your answer.

……
……
……
……
……
……

This the End of the Questionnaire

Thank you very much for your invaluable participation, contribution and information

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Ref No: **574455**

Date of Issue: **28/April/2020**

RESEARCH LICENSE

This is to Certify that Mr. FARAI TARUVINGA of University of Nairobi, has been licensed to conduct research in Nairobi on the topic: Emerging cyber security threats: A comparative study of Kenya and Zimbabwe, for the period ending: 28/April/2021.

License No: **NACOSTI/P/20/4803**

574455

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Verification QR Code

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

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 any rights thereunder are non-transferable
3. The Licensee shall inform the relevant County Director of Education, County Commissioner and County Governor before commencement of the research
4. Excavation, filming and collection of specimens are subject to further necessary clearance from relevant Government Agencies
5. The License 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 (thesis) within one 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 off Waiyaki Way, Upper Kabete,
P. O. Box 30623, 00100 Nairobi, KENYA
Land line: 020 4007000, 020 2241349, 020 3310571, 020 8001077
Mobile: 0713 788 787 / 0735 404 245
E-mail: dg@nacosti.go.ke / registry@nacosti.go.ke Website: www.nacosti.go.ke

APPENDIX III: PLAGIARISM Report

EMERGING CYBER SECURITY THREATS: ACOMPARATIVE STUDY OF KENYA AND ZIMBABWE

ORIGINALITY REPORT

12%	8%	5%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	pdfs.semanticscholar.org Internet Source	1%
2	link.springer.com Internet Source	1%
3	Submitted to Mount Kenya University Student Paper	<1%
4	Submitted to Kenyatta University Student Paper	<1%
5	Submitted to American Public University System Student Paper	<1%
6	etd.fcla.edu Internet Source	<1%
7	Submitted to Eiffel Corporation Student Paper	<1%
8	John-Paul Banchani, Elrena Van der Spuy. "Bibliography on police and policing research in South Africa, 2000–2012", South African Crime	<1%

	Quarterly, 2016 Publication	
9	Submitted to Strathmore University Student Paper	<1 %
10	Submitted to Loughborough University Student Paper	<1 %
11	Submitted to Edith Cowan University Student Paper	<1 %
12	pmworldjournal.net Internet Source	<1 %
13	Submitted to University of Pretoria Student Paper	<1 %
14	europe.hkbu.edu.hk Internet Source	<1 %
15	Submitted to Mesa State College Student Paper	<1 %
16	cadmus.eui.eu Internet Source	<1 %
17	Submitted to Leeds Metropolitan University Student Paper	<1 %
18	rcv.gov.vn Internet Source	<1 %
19	bazybg.uek.krakow.pl Internet Source	<1 %

20	Submitted to Kampala International University Student Paper	<1 %
21	Submitted to University of Southampton Student Paper	<1 %
22	www.scribd.com Internet Source	<1 %
23	Submitted to University of Birmingham Student Paper	<1 %
24	seminar.net Internet Source	<1 %
25	www.rsisinternational.org Internet Source	<1 %
26	journals.scholarpublishing.org Internet Source	<1 %
27	projectclue.com Internet Source	<1 %
28	journals.sagepub.com Internet Source	<1 %
29	cgch.lshtm.ac.uk Internet Source	<1 %
30	Submitted to University of Warwick Student Paper	<1 %
31	Submitted to De Montfort University Student Paper	<1 %

32	scindeks.ceon.rs Internet Source	<1 %
33	dspace.ut.ee Internet Source	<1 %
34	pure.royalholloway.ac.uk Internet Source	<1 %
35	Submitted to Royal Holloway and Bedford New College Student Paper	<1 %
36	"Facing Global Environmental Change", Springer Science and Business Media LLC, 2009 Publication	<1 %
37	journals.euser.org Internet Source	<1 %
38	Submitted to University of Abertay Dundee Student Paper	<1 %
39	www.tandfonline.com Internet Source	<1 %
40	Submitted to Macquarie University Student Paper	<1 %
41	etd.ohiolink.edu Internet Source	<1 %
	Submitted to University of Cambridge	

42	International Examinations Student Paper	<1%
43	swisstransparency.ch Internet Source	<1%
44	Cyber-peace.org Internet Source	<1%
45	Submitted to University of Maryland, University College Student Paper	<1%
46	graduatebusiness.albany.edu Internet Source	<1%
47	www.ajes.ro Internet Source	<1%
48	eprints.lse.ac.uk Internet Source	<1%
49	istheory.byu.edu Internet Source	<1%
50	Submitted to Leiden University Student Paper	<1%
51	Submitted to Kisii University Student Paper	<1%
52	Eneken Tikk-Ringas. "Chapter 8 Legal Framework of Cyber Security", Springer Science and Business Media LLC, 2015	<1%

	Publication	
53	www.nature.com Internet Source	<1 %
54	Submitted to Islamic Studies College (Qatar Foundation) Student Paper	<1 %
55	Submitted to American Intercontinental University Online Student Paper	<1 %
56	www.chathamhouse.org Internet Source	<1 %
57	Submitted to Chester College of Higher Education Student Paper	<1 %
58	Submitted to Istituto Marangoni LTD London Campus Student Paper	<1 %
59	Submitted to Grand Valley State University Student Paper	<1 %
60	theses.ubn.ru.nl Internet Source	<1 %
61	www.inderscienceonline.com Internet Source	<1 %
62	Submitted to University of Keele Student Paper	<1 %

63	Submitted to The Chicago School of Professional Psychology Student Paper	<1%
64	erepository.uonbi.ac.ke Internet Source	<1%
65	Peter D. Linquiti. "The Public Sector R&D Enterprise", Springer Science and Business Media LLC, 2015 Publication	<1%
66	library.college.police.uk Internet Source	<1%
67	repository.out.ac.tz Internet Source	<1%
68	Submitted to Curtin University of Technology Student Paper	<1%
69	Submitted to Midlands State University Student Paper	<1%
70	Submitted to University of Bristol Student Paper	<1%
71	"African Data Privacy Laws", Springer Science and Business Media LLC, 2016 Publication	<1%
72	www.serianu.com Internet Source	<1%

73	ir.canterbury.ac.nz Internet Source	<1%
74	ccdcoe.org Internet Source	<1%
75	Submitted to University of Westminster Student Paper	<1%
76	Submitted to Mancosa Student Paper	<1%
77	Submitted to South African National War College Student Paper	<1%
78	www.citethisforme.com Internet Source	<1%
79	Submitted to University of Strathclyde Student Paper	<1%
80	de.slideshare.net Internet Source	<1%
81	Submitted to Sim University Student Paper	<1%
82	gcsp.ch Internet Source	<1%
83	Submitted to Kaplan University Student Paper	<1%

84	Submitted to University of Portsmouth Student Paper	<1%
85	Submitted to Imperial College of Science, Technology and Medicine Student Paper	<1%
86	publications.polymtl.ca Internet Source	<1%
87	Submitted to Federal University of Technology Student Paper	<1%
88	Submitted to Nanyang Technological University, Singapore Student Paper	<1%
89	Submitted to Bahcesehir University Student Paper	<1%
90	Submitted to OTHM Qualifications Student Paper	<1%
91	Submitted to Laureate Higher Education Group Student Paper	<1%
92	www.dtic.mil Internet Source	<1%
93	escholarship.org Internet Source	<1%
94	Submitted to University of Leicester Student Paper	<1%

95	Submitted to Taylor's Education Group Student Paper	<1%
96	wwwisis.unam.na Internet Source	<1%
97	www.rusi.org Internet Source	<1%
98	Submitted to Women's University Student Paper	<1%
99	Submitted to University of St Andrews Student Paper	<1%
100	Submitted to American University of Nigeria Student Paper	<1%
101	Submitted to Higher Education Commission Pakistan Student Paper	<1%
102	cainscrossing.org Internet Source	<1%
103	Submitted to City University Student Paper	<1%
104	Charlotte Gill, Julie Hibdon, Cynthia Lum, Devon Johnson, Linda Merola, David Weisburd, Breanne Cave, Jaspreet Chahal. "“Translational Criminology” in action: a national survey of TSA's Playbook implementation at U.S. Airports", Security Journal, 2019	<1%

	Publication	
105	Submitted to Harrisburg University of Science and Technology Student Paper	<1%
106	hdl.handle.net Internet Source	<1%
107	uppolice.up.nic.in Internet Source	<1%
108	Submitted to College of Europe Student Paper	<1%
109	repository.up.ac.za Internet Source	<1%
110	Submitted to Ghana Technology University College Student Paper	<1%
111	nsfdc.nic.in Internet Source	<1%
112	nurt9jageneral.blogspot.com Internet Source	<1%
113	Submitted to RDI Distance Learning Student Paper	<1%
114	Submitted to UT, Dallas Student Paper	<1%
115	eera-ecer.de	

	Internet Source	<1%
116	ir.jkuat.ac.ke Internet Source	<1%
117	docshare.tips Internet Source	<1%
118	Submitted to University of Sunderland Student Paper	<1%
119	pt.scribd.com Internet Source	<1%
120	Submitted to Monash University Student Paper	<1%
121	Submitted to Fort Valley State University Student Paper	<1%
122	Submitted to Intercollege Student Paper	<1%
123	Submitted to Saint Paul University Student Paper	<1%
124	Submitted to Universita' di Siena Student Paper	<1%
125	Submitted to Masinde Muliro University of Science and Technology Student Paper	<1%
	"Current and Emerging Trends in Cyber	

126	Operations", Springer Science and Business Media LLC, 2015 Publication	<1%
127	Submitted to University of Nottingham Student Paper	<1%
128	Daniel R. McCarthy. "Power, Information Technology, and International Relations Theory", Springer Science and Business Media LLC, 2015 Publication	<1%

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		