UNIVERSITY OF NAIROBI

INSTITUTE DIPLOMACY AND INTERNATIONAL STUDIES

International Inter-Agency Coordination of State and Non-State Actors in Combating Global Cyber threat: Case Study of Kenya and Zambia

ROBERT ANTONY KINYUA KOBIA

SUPERVISOR: DR. PATRICK MALUKI

A research Project submitted in partial fulfillment of the requirements for the award of a Master of Arts degree in International Studies at the Institute of Diplomacy and International Studies, University of Nairobi.

November 2021

DECLARATION

This research project report is my original work and has not been submitted for an award to any other University or institution of higher learning

Signature: **Date**09/11/2021

Robert Antony Kinyua Kobia

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

Signature: **Date**29/11/2021

Dr. Patrick Maluki

University of Nairobi

Acknowledgments

I foremost wish to thank the Almighty God for guiding me throughout this process. I also wish to thank my supervisor DR. Patrick Maluki for his vigilant supervision and valuable comments in this entire process of the dissertation. I would also like to thank my family for their continuous support in the course of my studies. Finally, I am highly indebted to my friends, acquaintances, and colleagues for the moral support they have accorded me to ensure that I achieved my education goals.

Abstract

This research paper seeks to expound on the International Inter-Agency Coordination of State and Non-State Actors in Combating Global Cyber Security, focusing on Kenya and Zambia. There has been a rise in cybercrimes worldwide, including in developing nations such as Kenya and Zambia. This has hence forced nations to establish new strategic measures that can help in combating the increasing challenges in Cyber Security. The study identifies the role of both the government and non-government bodies in the policymaking processes regarding Cyber Security. It seeks to identify the most relevant and suitable recommendations and best policies for combating cybercrimes that can be enacted. The research paper has a detailed description of the issues, research questions, and a literature review. It also has a descriptive research methodology section, where the methods of data collection and analysis are identified. The statement of the problem and the theoretical framework of the research are highlighted and study's objectives are analyzed. Finally the findings from the entire research process are noted down followed by the recommendations for the identified gaps.

List of Acronyms and Abbreviations

AU- African Union

CA- Communications Authority

CIRT-Critical Incident Response Team

EAC- East African Community

EACO -The East African Communications Organization

FBI- Federal Bureau of Investigation

ICT-Information and Communications Technology

Interpol-The International Criminal Police Organization

KDF- Kenya Defense Forces

NGO- Non-Governmental Organization

NIS- The National Intelligence Service

SADC- Southern African Development Community

SME- Small and Medium-Sized Enterprises

UNCTAD-United Nations Conference on Trade and Development

USA- United States of America

USB-Universal Serial Bus

IBM – International Business Machines Corporation

TESPOK - Technology Service Providers of Kenya

ODPP – Office of the Director of Public Prosecution

CBK – Central Bank of Kenya

CIPIT - Centre for Intellectual Property and Information Technology

ROEA – Regional Office East Africa

BAKE – Bloggers Association of Kenya

CoE – Council of Europe

WEF – World Economic Forum

DRD – Data Retention Directive

CCK – Communication Commission of Kenya

AUC – African Union Commission

GDPR – General Data Protection Regulation

CISO – Cyber and Information Security Officer

CBN – Central Bank of Nigeria

NCRP – National Central Reference Points

FIC – Financial Intelligence Centre

WSIS – World Summit on the Information Security

ZICTA – Zambia Information and Communications Technology Authority

HARID – Home Affairs Research and Information Development

CJEU – European Court of Justice

Table of Contents

Chapter One

1.1 Background of the study

In the era of advanced technology, there has been a rise in the cases of cybercrimes across the globe, including in developing nations such as Kenya and Zambia. Cybercrime can be described as an activity where computers or networks are a tool, target, or path of criminal activity. According to Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism, cybercrime is described as acts with respect to cyber systems.[1] Some definitions try to take objectives or intentions into the account and define cybercrime more precisely, including cybercrimes being computer-mediated activities that are either illegal or considered illicit by certain parties which can be conducted through global electronic networks.[2] There are numerous ways in which persons can commit cybercrime. For example, when a person produces a USB device that contains malicious software, which can be used to destroy data on the computers, commits a crime, which is defined by Article 4 of the convention of cybercrime.

As more people are getting online, cyberspace is becoming a defining feature of modern life, where people and communities are socializing and organizing themselves across national borders and traditional socio-cultural boundaries. Nevertheless, cyber security is one of the greatest threats which have been brought about by the increased use of cyberspace.[3] "Cyber threats are not only increasing in scope and scale, they are also becoming increasingly difficult to investigate. Cyber criminals often operate through online forums, selling illicit goods and services,

[1] Sofaer, A. D., Grove, G. D., & Wilson, G. D. (2001). Draft International Convention To Enhance Protection from Cyber Crime and Terrorism. *The Transnational Dimension of Cyber Crime and Terrorism*, 249-265.

[2] EUROPOL. (2011). *The Changing Face of Cybercrime.* Retrieved from https://www.europol.europa.eu/newsroom/news/changing-face-of-cybercrime

[3] Jakobi, A. P. (2013). Non-State Actors All Around: The Governance of Cybercrime. 129-148. doi:https://doi.org/10.1057/9781137334428_7

including tools that can be used to facilitate cyber-attacks. "[4]Non-state actors have a very key role to play in helping retain cyber security, both on a large and small scale and most likely players in the future of the full-scale cyberwar. In the event of cyber-attacks, the government tends to seek the help of non-state actors who can help in averting the attacks or reducing the number of risks associated with the crimes.

In the last two decades, rogue malware authors and organized cybercriminals have been on a rise, a factor which has been attributed primarily by their need for economic gains. An example was in 2009, where Ghost Net had access to confidential information belonging to both government and non-governmental firms in over 1000 nations across the globe[5]. There were claims that Ghost Net belonged to the Chinese government, a claim that the government denied. It was just one of the many examples of individuals, systems, and parties who have ventured into cybercrime. This has hence become a major priority for many stakeholders, both in and out of government, as a way of protecting members, governments, and institutions against such attacks which are increasing by the day.

Both the government and non-government bodies are involved in the policymaking processes, where through their suggestions, researches and recommendations for the best policies for combating cybercrimes can be enacted.[6] Some of the non-government bodies involved in such processes include; the civil society, academia, and the private sector who have continually engaged on the matter. In the case of Kenya, the general public is another party that can be engaged through

[4] Federal Bureau of Investigation. (2017). Roles and Responsibilities for Defending the Nation from Cyber Attack. Retrieved from https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities

[5] Sigholm, J. Non-State Actors in Cyberspace Operations. *Swedish National Defence College, Sweden*. (2016): doi:https://doi.org/10.1515/jms-2016-0184

[6] SAMBULI, N., MAINA, J., & KAMAU, T. Mapping the Cyber Policy Landscape: Kenya. (2016): Retrieved from https://www.gp-digital.org/wp-content/uploads/2016/12/Kenya-Cyber-Policy-Mapping-final-i-1.pdf

the public consultation phase that is treasured as a national value and, obligatory step in the legislative process which is guaranteed by the constitution. Both Kenya and Zambia have a number of laws, regulations, and policies that pertain to curbing cyber security, where they also involve the protection and safeguarding the rights of its citizens[7]. Kenya, for example, has bills such as the 2016 computer and Cybercrimes Bills, which in its "Memorandum of Objects and Reasons" that it does not contain provisions that limit the rights and fundamental freedoms[8]. This means that the current laws and regulations in place, still have a gap, more so concerning human rights principles, a factor that should be considered in future legal frameworks.

Both Kenya and Zambia, are examples of developing nations that have been prone to a diverse range of cyber threats and challenges that which are as a consequence of the advancement and ubiquity of IT. Several legal frameworks have emerged as a result of these technological developments.[9]The governments in the two nations recognize this, and in Kenya, for example, the government is in the process of developing and reviewing various legislative frameworks and institutions which will aid in equipping them with mechanisms of addressing cyber security in the nation.

There is therefore a need for an in-depth study on the issue of cybercrime. From the study, the interagency coordination between both state and non-state actors will be comprehensively analyzed. This will help in determining the current relationships amongst the actors in place, and how they have been, in identifying sustainable solutions on the issues of cybercrimes. The challenge faced by both actors in the war against cybercrime is another critical topic that will

[7]SAMBULI, N., MAINA, J., & KAMAU, T. Mapping the Cyber Policy Landscape: Kenya. (2016): Retrieved from https://www.gp-digital.org/wp-content/uploads/2016/12/Kenya-Cyber-Policy-Mapping-final-i-1.pdf

[8] Ibid

[9]Ibid

comprehensively be investigated. The major focus will be mostly on the cases of Kenya and Zambia, which are both developing nations and have in the past undertaken different measures in place to tackle the challenge of cybercrime in their respective nations. This study will seek to identify the various gaps in the fight against the cybercrimes in these respective nations, and understand the role of the state and non-state actors, where it will conclude by identifying more long-lasting solutions to the identified issues.

1.2 Statement of the Problem

Currently, there is more advanced internet infrastructure, a growing number of internet users and widespread use of electronic banking and payment systems. There is a growing threat, which has made this a worldwide phenomenon and a priority of many nations' agenda. This has also been a result of the increasing availability of wireless internet access points and hotspots, where it is easy for users to expose their personal data. These are some of the most targeted points, where criminals easily use open-access internet connections to mask online activities that the account holders could later be held liable. This is a major challenge faced by many nations, in the war against cybercrimes. As a result of the increasing cases of cybercrimes, the major challenges faced are the lack of a healthy relationship and coordination between the state and non-state actors in combating global security. There is hence a need to have a well-laid strategy about how both the state and non-state actors should approach this issue and develop the best mechanisms that will help deal with the crimes. Since the crimes occur across the borders, a more concerted effort by the international community is needed to deal with it.

Many institutions both private and public are unable to understand the extent to which cybercrimes affect the businesses and structures in place. Cyber insecurity tends to affect the performances and excellence of these institutions, making them very vulnerable to external attacks.[10]Theft or disablement of any of the systems can lead to weakening and destruction of business and structures, which can be seen from the most recent high-profile attacks across the globe.

1.3 Research Questions

To achieve the set objectives, the research will seek to address the following research questions:

i. What is the current state of international inter agency coordination amongst all the relevant actors in cybercrime prevention in both Kenya and Zambia?

ii. Which measures have the government and other non-state actors undertaken as way of mitigating Cybercrimes?

iii. What are the challenges faced both by the state and non-state actors in their collaboration in the fight against cybercrimes and ensuring sustainable cybersecurity policies?

1.4 Objectives of the study

The objectives of the study are to:

i. examine the current state of international, inter agency coordination amongst all the relevant actors in cybercrime prevention in both Kenya and Zambia

ii. evaluate the measures taken by the government and other non-state actors to mitigate cybercrimes.

[10] Telecommunication Development Sector. (September, 2012). UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

iii. critically analyze the challenges faced both by the state and non-state actors in their collaboration in the fight against cybercrimes and ensuring sustainable cybersecurity policies.

1.5 Literature Review

1.5.1 Introduction

Multiple studies have been conducted on the contentious topic of cybercrimes, the role of multiple agencies, and how different countries undertake various roles in ensuring that they have structures in place. The literature review section is very critical for this research in that it will analyze and evaluate various literature on the subject matter., The gaps and necessary findings will be used for the discussion and conclusions for the study. The literature review also lays the foundation for the study, through identifying facts, statistics, and any necessary information which is line with the goals and objectives of the study. The review covers all the crucial aspects of cybercrimes across the globe, with the main target being Kenyan and Zambia, which are two of the developing nations in Africa. It will focus on parts scholar articles on how the inter-agencies have helped in developing sustainable solutions to the challenge of cybercrimes, and areas which they are yet to pursue.

Existing literature expounds the issue of cybersecurity, crimes, and the role of both state and non-state actors on ensuring that there is enhanced cybersecurity in nations. However, from different pieces of literature, it is apparent that the technical complexities of cybersecurity are often not understood, even by different personnel in the security business. [11]The complexity of

[11] Singer, Peter W., and Allan Friedman. *Cybersecurity: What everyone needs to know*. oup USA, 2014.

cybersecurity is much bigger than in other domains, hence the challenges involved in addressing it.

According to Thomas J. Holt, Cybercrimes takes many forms. It may take place through cyber trespass effected by computer hacker for malicious or ethical purposes. In this case hackers engage in and develop tools that destroy computers, deface communication sites such as websites and introduces malwares that have devastating effects on the computers. Cyber deception, fraud and theft are other ways the crimes take effect. Digital piracy and abuse of copyrights are frequent. Cyber space is also being corrupted as phonographic materials which are easily accessible inflicting negative impacts to the society's moral fabric[12]. Cyber bullying is becoming common too. the study noted that most traditional judicial systems worldwide have not been able to deal with these issues of cybercrime.

1.5.2 Theoretical Framework

The study incorporates the criminal justice theories and biological theory of crime in order to explain more about the cyber-crime and the ways against such crimes. The reason for integrating these theories into the research is due to their accuracy and relation with most critical issues regarding cyber insecurities across the region. This will also help in the provision of sustainable solutions likely to help in combating such crimes. The two theories also aid to further comprehend how the actions of these perpetrators can get detected and avoided through undertaking interventions from both state and non-state actors. The criminal justice theories help in analyzing then criminal behaviors of the cyber space offenders, where it links the crime to the

[12] Telecommunication Development Sector. September, 2012. "UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE." http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

shifting paradigm in technology. The criminal justice theories, also expound on the role of governments and other actors in dealing and prevent such crimes. To complement the criminal justice theories, there is need to incorporate the biological theory of crime, which explores on the biological nature of human beings and their need to commit the crime.

Leaders across the globe have continually expressed their worry and concerns about growing cybersecurity threats. President Obama when in power declared that "cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century."[13] His position has been repeated by many other leaders from both developed and developing nations meaning that it is an issue that calls for more action. President Kenyatta of Kenya has also been very vocal on the need for having more stringent cybersecurity measures, where he signed into law the Computer and Cyber-Crimes Bill 2018 into law. This is one of the laws which spell out stiff punishment to cybercriminals.[14] The laws also provide for timely and effective detection, prohibition, prevention, response, investigation, and prosecution of computers and cybercrimes.

The law seeks to protect the citizens, where it deals with offenses relating to the computer systems, including but not limited to unauthorized access, interference, interception and disclosure of password cyber espionage, publications, cyber terrorism, child pornography, and wrongful distribution of intimate and obscene images. Failure to observe the laws to the later, according to the bill, could land one in jail for at least five years or get fined millions of shillings. The bill signed by the president was one of the ways of providing necessary frameworks, which would help

[13] Ibid

[14] Citizen TV. (2018). Ksh.5M fine or 2 years in jail for fake news as Uhuru signs Cyber-Crimes Bill. Retrieved from https://citizentv.co.ke/news/ksh-5m-fine-or-2-years-in-jail-for-fake-news-as-uhuru-signs-cyber-crimes-bill-200524/

in the prevention and controlling of cybercrimes and other cyber offenses in the country. In a survey conducted to determine the state of the globe in the near future according to Singer & Friedman(2014), the foreign magazine describes the cyber areas as the single greatest emerging threat. [15]According to the Boston Globe, the future was already here, meaning that the world had to embrace itself to deal with the threat, where it was referred to as the cyber world war.

1.5.3 Role of the Government in combating Cyber-Crime

The government is the main stakeholders that is concerned with the issue of Cyber Security, because of its mandate to protect the citizens and business. The government also has the required resources that can help in the creation of structures and processes that can help in ensuring that cybersecurity is well tackled. Through the government, it is also relatively easier to enact the required laws and regulations that can protect various parties, institutions, and personnel from attacks[16]. As a result of cybercrimes, governments across the world have resulted in creating numerous offices and bureaucracies of dealing with the threat. The US department of homeland security's National cybersecurity Division, for example, doubles or triples every year since its inception as a way of ensuring that it is ready to deal with the rapidly emerging cases. The same is true for armed forces around the globe like the US Cyber Command and the Chinese "Information Security Base" new military units whose very mission is to fight and win wars in cyberspace. [17] These aspects of cyber stuff erase real risks; nevertheless, how they respond to such risks is more crucial to the future. By losing confidence in the safety and security of the internet,

[15] Singer, P. W., & Friedman, A. 2014. Cybersecurity and Cyberwar What Everyone Needs To Know. Oxford University Press.

[16] Lewis, James A. "Sovereignty and the Role of Government in Cyberspace." *Brown J. World Aff.* 16 (2009): 55.

[17] Sofaer, A. D., Grove, G. D., & Wilson, G. D. Draft International Convention to Enhance Protection from Cyber Crime and Terrorism. The Transnational Dimension of Cyber Crime and Terrorism, (2001):249-265.

then there will be a retreat for cyberspace. The cybersecurity fears may lead to a compromised notion of privacy, a factor which can affect the major efforts associated with the integration of the internet in our daily promise hence leading to an undermining of the economic and human rights benefits experienced from global connectivity.

Nevertheless, the incorporation of the non-state actors can help in guiding the government and the creation of innovative systems that can help with the tackling of cybercrimes. [18]Non-state actors together with the government can effectively work hand in hand in addressing the best strategic measures of dealing with cyber insecurity. The most common actors in cyberspace are ordinary citizen, who use the internet for lawful purposes such as browsing the web. Ordinary citizens range from employees of companies, organizations, and the government.[19] Employment of non-state actors into the cyberspace is an attractive option, more so when pursuing limited strategic goals. Incorporating these actors will help the government in various aspects and also ensure that everyone is involved in the war against cybercrimes, through collaborations.

1.5.4 Collaboration of state and non-state actors in fighting cyber-Crime

It is the role of both the government and other non-state actors to take part in protecting their countries and citizens against cybercrimes. More than any other crimes, the governance of cybercrime is more on private actors than on the state actors. This creates conflict of interest on the two parties.[20]Both state and non-state actors are imperative components of global crime governance. Historically, the state actors have been left in charge of traditional crime such as drug related crimes, slavery and other professional law enforcement amongst others.[21]

[18]Jakobi, A., & Wolf, K. (2013). Non-State Actors All Around: The Governance of Cybercrime. *The Transnational Governance of Violence and Crime. Governance and Limited Statehood*. doi:https://doi.org/10.1057/9781137334428_7

[19] Ibid

[20] Ibid, 130.

[21] Ibid.

In recent years, non-state actors have also become an important element in the implementation of crime governance, in part by providing data about offenses that governmental actors would have difficulty in collecting alone."[22] Nonetheless in the case of cybercrimes, both the state and the non-state actors have a critical role to play in the implementation of crime governance, where non state actors can help in the provision of data that the government officials would have difficulties in collecting alone. The interplay of public and private actors is important to find effective ways of governing cybercrime.

The relationship between the state and non-state actors varies across issues and areas. The recent efforts of controlling cybercrime require new approaches. This so given the fact that there is a twist in its global dimension and the significant difficulties for the state actors to prosecute such crimes.[23] It is evident that in the pursuit of addressing cybercrimes, the private actors play a significant role since they help in the addressing the cybercrime regulations despite the fact that state-driven crime and the cyber warfare is growing concern. [24]Many governments are left with no choice but to integrate the private business, such as internet service providers who can help in combating the crimes. The interplay between the state and non-state actors is crucial in that it helps in finding effective ways of governing cybercrime. The regulation of cybercrime is a crucial example of the need for both state and non-state actors for working together in the regulation of cover areas such as security.

[22] Jakobi, A. P. Non-State Actors All Around: The Governance of Cybercrime. (2013): 129-148. doi:https://doi.org/10.1057/9781137334428_7

[23] Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, *4*(1), 1-37.

[24] Sigholm, Johan. 2016. "Non-State Actors in Cyberspace Operations." *Swedish National Defence College, Sweden.* doi:https://doi.org/10.1515/jms-2016-0184.

In the last few years, rogue malware authors and organized cybercriminals have been on a rise, a factor which has been attributed primarily by their need for economic gains. An example was in 2009, where Ghost Net had access to confidential information belonging to both government and non-governmental firms in over 1000 nations across the globe. There were claims that Ghost Net belonged to the Chinese government, a claim that the government denied. It was just one of the many examples of individuals, systems, and parties who have ventured into cybercrime. This has hence become a major priority for many stakeholders, both in and out of government, as a way of protecting members, governments, and institutions against such attacks which are increasing by the day.

Both the government and non-government bodies are involved in the policymaking processes, where through their suggestions, researches, and recommendations for the best policies for combating cybercrimes can be enacted. [25]Some of the non-government bodies involved in such processes includes civil society, academia, and the private sector who have continually engaged in the matter. In the case of Kenya, the general public is another party that can be engaged through the public consultation phase that is treasured as a national value and, obligatory step in the legislative process which is guaranteed by the constitution. Both Kenya and Zambia have a number of laws, regulations, and policies that pertain to curbing cybersecurity, where they also involve the protection and safeguarding the rights of its citizens.[26] Kenya, for example, has bills such as the 2016 computer and Cybercrimes Bills, which in its "Memorandum of Objects and Reasons" that it does not contain provisions that limit the rights and fundamental freedoms.[27]This means that the

[25] Ibid

[26]SAMBULI, NANJIRA, JULIET MAINA, and TYRUS KAMAU. 2016. "Mapping the Cyber Policy Landscape: Kenya." https://www.gp-digital.org/wp-content/uploads/2016/12/Kenya-Cyber-Policy-Mapping-final-i-1.pdf.

[27] Ibid

current laws and regulations in place still have a gap, more so concerning human rights principles, a factor that should be considered in future legal frameworks.

1.5.5 Need for government involvement

Given the magnitude of the effects of cybercrimes on a nation, there is a need for massive government involvement in establishing minimum standards for security. The involvement of governments in enacting cybersecurity measures can help instill confidence in the citizens, and ensure that their private information is secured. Through laws, the government is also able to ensure that vendors are liable for delivering secure products and services. The role of the government is to lead by example in the area of cybersecurity.[28]The government systems are funded by the taxpayers, monies, meaning that the monies should be appropriately used in ensuring that there is excellence in the area of cybersecurity.

However, currently many governments across the world have failed to analyze this challenge and create solutions to their citizens, hence failing to provide basic cybersecurity hygiene. There have also been minimum collaborations between the government and non-state actors, which would help develop innovative strategies that will help curb the challenge of cybercrimes currently. "If governments want to realize the savings and efficiencies from going digital, they need to constantly keep one step ahead of criminals. "[29] The governments need to set an example by getting accountable for providing basic cyber hygiene.

[28] Gilligan, J. M. (2017). The Government Role in Improving Cyber Security. Retrieved from https://www.globalcyberalliance.org/the-government-role-in-improving-cyber-security/

[29] KPMG. (2016). Five ways for governments to tighten up cyber security. Retrieved from https://home.kpmg/xx/en/home/insights/2016/05/five-ways-for-governments-to-tighten-up-cyber-security.html

1.5.6 Players in cyber security across the globe

The global inter-agency coordination between the various actors has also had a huge gap that ought to be addressed in the near future as a way of ensuring that the cases of cyber insecurities in nations across the globe are addressed. In the past few years, there have also been multiple global conventions and conferences among both governmental and non-government stakeholders with an aim of addressing the issue of cybersecurity and the best measures that can be used to address the issue.[30] Nevertheless, despite these conferences, it is apparent that there have been lapses in the implementation of best measures that could be undertaken by various players both within and out of the government. There will, therefore, be a need to assess the outcomes of these conventions and conferences, and understand the challenges faced in the implementation process of the agreed measures. The technology has been advancing over the years, so have been the cybercrime strategies. The changes in the ways of committing the crimes have constantly challenged the bodies mandated with dealing with the crimes, due to its changing nature. The changing trends in the ways cyber-crimes are committed are attributed to the advancements in the use of technology.

The governments have the capability of protecting the issue of the ICTs in committing a crime through the use of the legislative bodies, who enact the laws, and the judiciary, which undertaken the role of prosecuting and punishing the criminals. It is relatively easier to fight cybercrime through harmonization of legislative approaches and coordination of actions, which can help in the investigation and prevention of cybercrime at different levels, i.e. internationally, nationally, and regionally. Cooperating with the private sector is another key responsibility of the government in the efforts of combating crime. This includes the development of the tools for

[30] Ibid

effective cooperation with the industry, where it can encourage the application of co-regulation and self-regulation tools. Nevertheless, there is a need to establish that every actor in this multi-sector environment of fighting and preventing cybercrimes faces numerous challenges. Some of the challenges include the general changes that merge due to the global nature of the internet of unique series related to the nature of the duties, and the functions used to operate the real world in addressing cybercrime.

1.5.7 How other countries have handled cyber security

In the African region, the African Union member states adopted in 2014 the African Union Convention on Cyber Security and personal data protection as a legal framework to build the information society.[31] The convention was keen to mobilize all public and private actors (states, local communities, private sector enterprises, civil society organizations the media training and research institutions among others) for the promotion of Cyber security.

According to a recent report, the government agencies rank last on matters of cybersecurity as compared to the private industries.[32] In the United States, the federal government has more than 77,000 data breaches in the year 2015, which a 10% increased from 2014. Based on the figures it is apparent that government targeted ransomware is on the rise. According to Bit sight, a leading cybersecurity rating company, there are ransomware attacks on government agencies globally that have tripled in 2015.[33] Based on the report, it is apparent that the government scored lowly

[31] Sofaer, Abraham D., Gregory D. Grove, and George D. Wilson. 2001. "Draft International Convention To Enhance Protection from Cyber Crime and Terrorism." *The Transnational Dimension of Cyber Crime and Terrorism* 249-265.

[32] Careers in cyber security. 2019. *Cyber Security and Its Role in Government. How Government Can Combat Cyber Threats.* https://careersincybersecurity.com/cyber-security-and-its-role-in-government/.

[33] Ibid

concerning cybersecurity as compared to other industries, and scored the highest ransomware attack rates. This is so since the government has been one of the main victims of data breaches, which exposes its weaknesses in network security, software patching, malware, and social engineering. Hackers have constantly used social engineering to obtain the credentials of a third-party contractor, where they then deploy a malware package. As a result, this has forced governments across the world to increase cybersecurity spending, as a way of ensuring that they can protect their systems against the threats. Another way of combatting cybercrimes is through the enactment of the legislation, such as the US congress cybersecurity act of 2015, which makes it easier for private companies to share cybersecurity information with the government. There is hence a need for the adoption of effective substantial criminal legislation and procedural instruments which allow for investigation and more understanding information and communication technologies.[34]

1.5.8 Fight against cybercrime in Africa

` Africa is one of the fastest-growing regions with regard to the use of the internet. It is also growing in terms of cybercrime activities. In the most recent case, the continent has also become one of the sources of cyberattacks that target the rest of the globe. A number of criminals targeting offshore accounts and institutions have been noted to come from several African nations.[35] Nevertheless, various measures have been taken by specific nations to address the issue of threats and ways of improving cybersecurity in the continent. Many nations within the continents have developed legislation through the lawmakers where they seek to fight the growing cyber-related crimes. A majority of the nations within the continent have also developed structures that will help

[34] Tropina, Tatiana. 2009. "Cyber-policing: the role of the police in fighting cybercrime." *European Police Science and Research Bulletin · Special Conference Issue Nr. 2.* Germany.

[35] Kshetri, Nir. "Cybercrime and cybersecurity in Africa." (2019): 77-81.

in strengthening the enforcement measures. The measures are taken both by the government and private sectors that have a key role to play in curbing the threat of cybercrime in the continent.

According to a report by the Ovumone, a British based consulting firm, by 2022, it is expected that more than a billion people will have access to the internet. This may mean that there may be a 10-15% increased rate of the levels of cybercrime-related activities such as hacking. Bulent Teksoz, of Symantec Middle East, believes that “Cybercrime is shifting towards the emerging economies. This is where the cybercriminals believe the low-hanging fruit is”. As a result, many African nations have become both important sources and also victims of cyber threats. According to a research by a Kenyan based IT and business advisory firm Serianu, Africa lost up to $3.5 billion to cybercrime in 2017 alone.[36] In that year alone Kenya alone lost $210 million, whereas Nigeria lost around $649 million.[37] South Africa on the other hand, according to the South African Banking Risk Information Centre, loses around $157 million annually, as a result of cyberattacks. This shows how serious the case of cyber-attacks is facing economies not just globally, but also in African nations.

It is evident that cybercriminals are viewing Africa as a safe haven, when they can operate illegally, without getting noticed. According to a Symantec report in 2014, cybercrime in Africa was increasing at a higher rate than any other region in the world. This is in terms of, malware, emails, hacking of accounts, and cases related to botnets. Some economies in the continent are more attractive to cybercriminals, as a result of the high degree of digitalization of economic

[36]

SERIANU. 2017. "Africa Cyber Security Report 2017." *Demystifying Africa Cyber Security Poverty Line.* https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf.

[37] Ibid

activities. Some of the activities are most attractive to cybercriminals include online banking services, mobile banking, and other online related services, where the perpetrators tend to hack and gain access to lump sums of money. For example, in South Africa alone, 86% used online banking services, a proportion which is higher than many nations including Turkey and the Middle East. [38] A major reason for the numerous cyber-attacks in the continent is, majorly due to the vulnerable systems in place, which are unable to detect or prevent incidences of cybercrimes. Secondly, many nations also have lax cybersecurity systems, hence giving criminals an easy time to undertake their illegal cyber-related activities without getting noticed. Libya and Zimbabwe are two of the world's highest software rates as of 2017.[39]

Many internet users in the continent also lack vital skills when using the internet and protect themselves from the rising cybersecurity threats. This makes it very easy for cybercriminals to target them. Just like in many other developing nations, the users are inexperienced and not technically savvy, a factor that increases the risk of attacks. It is also apparent that users in many nations in the continent have a shortage of cybersecurity manpower. [40]Many African nations have faced economic and institutional barriers that can help them boost their cybersecurity manpower. Some of the nation's lack well-laid policies that can also help protect citizens and institutions

[38] Chetty, R.-L. (2018). Kaspersky Lab report says South Africans most susceptible to online banking attacks. Retrieved from https://www.htxt.co.za/2018/11/12/kaspersky-lab-report-says-south-africans-most-susceptible-to-online-banking-attacks/

[39] BSA Global Software Survey. (June 2018). Software Management: Security Imperative, Business Opportunity. Retrieved from https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf

[40]

SERIANU. 2017. "Africa Cyber Security Report 2017." *Demystifying Africa Cyber Security Poverty Line.* https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf.

against cyber-related attacks. An example is Cameroon, where in 2016 was in the process of launching cybersecurity skill development programs, but feared that the trainees could use the skills gained to commit cybercrimes.[41]

Weak legislation and law enforcement could be another factor enhancing the upsurge of cyber-related crimes. Many nations in the continent have economies that are characterized by permissiveness or regulatory regimes, which lead to an environment that is futile ground for cybercrime activities. A high number of the nations in the continent lack specific legal provisions which can help in the fight against cybercrime, and also in dealing with electronic evidence.[42] In some nations, law enforcement officials fail to undertake any major actions against hackers who attack international websites. Some officials, for example in Nigeria, are accused of being ignorant of the high cases of cybercrimes originating from the country. Some of them are also reported to be part of the cybercrime cartels. This hence makes it difficult to effectively have a well-laid structure in some of the nations that can help to effectively tackle the threat of cybercrimes.

African nations must hence improve their strategies in order to ensure that they protect their citizens and institutions against the high threat of cyber-related crimes which is on an upsurge. First, there is a need to upgrade the technology and meet the international standards for the security of internet-related platforms and systems in place.[43] Nations also need to establish more laws which criminalize cyber-attacks and enable the law enforcers and police to be able to adequately

[41]Chimtom, N. K. (2016). CAMEROON'S DILEMMA IN FIGHTING CYBERCRIME. Retrieved from https://www.africanindy.com/business/cameroons-dilemma-in-fighting-cybercrime-5073265

[42] Ibid

[43]

SERIANU. 2017. "Africa Cyber Security Report 2017." *Demystifying Africa Cyber Security Poverty Line.* https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf.

investigate and prosecute any cybercrime-related activities.[44]Governments in place ought to have risk management policies, and regularly review security regulations for ICT. They also can help in expanding training to make sure that economies have the relevant human resources that will help have robust security programs.

1.5.9 Empirical Framework

Multiple journals and articles expound on the issue of cybersecurity. Nevertheless, according to Singer & Friedman, it should be understood that the rise of cybersecurity has emerged as a result of the growth in modern technology.[45] According to the author, the internet is no longer about sending mail or compiling information, but rather handling anything including electrical plants and household items. According to Cisco, a company that helps in ruining much of the back end of the internet estimated that there would be approximately 8.7 billion devices, which would be connected to the internet by 2012 and rise to over 409 billion by 2020. The Internet has been linked to devices such as fridges, doors medical devices, and various other gadgets. This shows that there has been a huge shift in paradigm concerning the use of modern technology in people's day to day activities.

There have been numerous reports of scores of attempted cyber-attacks on critical infrastructure to nations such as air traffic control systems, national electricity grids, satellite systems, and government structures. [46]According to multiple journals and publications, the attacks

[44] Ibid

[45] Singer, P. W., & Friedman, A. (2014). Cybersecurity And Cyberwar What Everyone Needs to Know. Oxford University Press.

[46]London Institute of Banking & Finance. 2017. "The changing face of Cybercrime." *A special report by The London Institute of Banking & Finance.* https://www.libf.ac.uk/docs/default-source/default-document-library/the-changing-face-of-cybercrime464f2e43ec86691782d0ff00001f97d9.pdf?sfvrsn=53c9478d_0.

on government systems have led to governments stressing on the need for stronger cyber defenses, as a way of protecting the governments and institutions from the attacks. They expound on the need for examining the current state of international, inter agency coordination amongst all the relevant actors in cybercrime prevention in both Kenya and Zambia.

According to the IBM cybersecurity Index, some of the most likely sectors to be targeted by hackers include financial services, health care, and manufacturing. This is due to the vast quantity of personal information and potential monetary gains associated with these fields. It is also estimated that by 2020, it is likely that 30 billion devices will be connected to the internet of things, which is a huge growth in devices, where multiple people will be connected, hence leading to a high potential for more cyber threats.[47] The cyber insurance industry, on the other hand, is estimated to be over $3billion, an industry which will provide a market mechanism for quantifying cyber risks and encouraging forms to improve their security. From the statistics, the study can be able to evaluate the measures that have been taken by the government and other state non actors, and how their actions help in the mitigation of cybercrimes.

One of the most promising future policies in the fight against cybercrime cyberspace is public and private partnerships. Multiple sources are of the opinion that the private sector actors have played a very domain role in driving the ICT sector development and innovation. They also possess the infrastructure and have direct access to it hence making them vital players in the role of fighting cybercrime. The sources are vital in expounding io the measures taken by the government and other non-state actors to mitigate Cybercrimes.

[47] Savage, Ed. 2019. "Tackling the challenges of cyber security." https://www.paconsulting.com/insights/tackling-the-challenges-of-cyber-security-the-role-of-government/.

1.5.10 Conclusion

From the multiple articles and journals on the topic of cybersecurity, it is manifest that there is a need to undertake a more in-depth study on the issue of the subject of cybercrime and security. The research will need to strictly focus more on the Inter-Agency Coordination of State and Non-State Actors in Combating Global Cyber Security. The key focus of the study will be Kenya and Zambia, which are both developing nations, and have made strides in the fight against cybercrime. The two nations also face multiple challenges in the fight. From the study, most suitable and sustainable solutions to the challenges will be investigated and identified, where they will help the agencies in developing better mechanisms and strategies in the fight against cybercrime. This research also seeks to explore the international conventions and the different types of players involved with identifying solutions to the issue of cybersecurity across the globe[48]. It seeks to expound on the significant obstacles of attaining effective arms control of the cyber domain and as a result identifying effective solutions to the underlying cybersecurity challenges. The study also seeks to investigate the roles of both the state and non-state agencies in combating global cybersecurity and how these actors are involved in the International Inter-Agency Coordination.

From the study, the role of each of the actors will be identified, where their roles in the future of ensuring that there is sustainability in cybersecurity will be comprehensively analyzed and discussed. The partnerships between the two sectors can either be through operational cooperation in particular areas or can be through long term campaigns.[49] Examples of the

[48]Jakobi, A. P. Non-State Actors All Around: The Governance of Cybercrime. (2013): 129-148. doi:https://doi.org/10.1057/9781137334428_7

[49] Ibid

partnerships that the two sectors can get into include cooperating in the training courses, setting up networks, sharing information of suspicious activities online, monitoring and blocking illegal content on the internet, and hosting conferences, conventions, and seminars to address sustainable solutions to the challenge of cybercrime.[50] These partnerships have in the past proven to be an effective way of ensuring the efficacy of addressing cyber-related threats and in the war against the crime.

1.5.11 Literature gaps

A major literature gap was the accessibility of the information regarding cybersecurity and cybercrime. Some of the documents are very sensitive and confidential and hence cannot be used in the evaluation of past studies. Accessing the document is not easy., this would require reaching out to crucial government departments for authorization. As much as there are multiple sources and materials on cybersecurity and crime, most of these sources provide only basic information regarding the subject matter and the coordination of state and non-state actors. There is hence a need to undertake a more in-depth study on the topic, and explore on most sustainable solutions that will help nations to overcome these growing challenges.

1.6 Justification

The purpose of this project is to examine the challenge of cyber-crime across the region, mainly focusing on Kenya and Zambia. Cybersecurity has been of great challenge. This has been attributed by the growth in the usage of the internet, where many persons have access to the internet either through social media, online transactions, or through mail services. The growing threat of cybercrime across the globe has prompted many individuals to undertake thorough research in the

[50] Vogel, J. (2007) Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico.

area, with the aim of ensuring that solutions to these challenges are identified. The more people spend online, the easier it is for the potential of fraudsters to access data. There are technical complexities of cybersecurity, which are not well understood by both the governments and non-government actors. Cybersecurity is a true system of system engineering problems whose complexity rivals' other domains. Consumers and citizens expect that both governments and other non-government actors they are affiliated to protect them against the harm and attacks associated with cybercrime. Many companies are investing in cybersecurity, but still cannot fully be able to protect their consumers without the help of the government, which helps in the facilitation of great systems and enactment of laws and regulations that protect the consumers[51].

Nevertheless, despite the efforts, there are still many products and services that face major security flaws and breaches. This is a major issue which means that there is a need for both the government and the other non-state actors to collaborate and work towards improving the state of cybersecurity. [52]Well laid government interventions and collaboration with the relevant actors will greatly help in addressing the issue and ensuring that the citizens, government, and non-government institutions have strong structures in place that will shield them from any related cybercrime.

The project also seeks to comprehensively analyze the policies and laws in place that help in governing the cyberspace of Kenya and Zambia. This is through identifying the laws enacted by the parliament, and how effective they have in the battle against cyber war. The research will also seek further measures that the governments could incorporate as way of ensuring that the people and institutions are protected against the increasing cases of cybercrimes. The data

[51]Caravelli, Jack, and Nigel Jones. 2019. *Cyber Security: Threats And Responses For Government And Business*. Praeger Security International.
[52] Ibid

collection process selected for this particular research is crucial in that it will help collect most critical data that will in turn help in acquiring most critical information regarding the subject of cyber criminals. In so doing, then the stakeholders' information, solutions and recommendations will be taken into account. The results will help institutions, both the state and non-state organizations in addressing the rising cases of crime in both Kenya and Zambia.

1.7 The Hypotheses

This study was based on the following hypotheses that:

a) Proper coordination and functioning of state and all relevant actors in combating cybercrime is paramount as opposed to lack of or poor coordination amongst all relevant actors.

b) If the measures taken by the government and other non-state actors in dealing with cybercrime are well implemented, then risks associated with cybercrime will be low.

c) The challenges occurring due to collaboration of state and non-state actors in their fight against cybercrime will have negative impacts in creating and ensuring sustainable cyber security policies.

1.8 Methodology of the Research

1.8.1 Introduction

To attain the study's set goals and objectives, there was a need to undertake in-depth research. This entailed undertaking in-depth interviews, where persons conversant with the topic of the study were consulted and engaged, with an aim of ensuring that they provided detailed information regarding Cybercrimes and cybersecurity. The respondents were also approached to provide potential solutions that both the government and Zambia can utilize to fight against cybercrime.

Qualitative research method was used for the study due to its multiple advantages such as it would ensure that cybercrime is comprehensively addressed. The research also made use of purpose non-probability sampling. Semi-structured, online surveys were conducted, where data analysis was done through the use of thematic content analysis. All the participants who undertook part in the study had to have prior knowledge and vast experience in cybercrime and cyberwar to ensure that their responses were in line with the set goals and objectives. Ten participants who were selected for the interview were only those with vast experience and prior knowledge of criminology and cybersecurity matters.

1.8.2 Study design

In this research, there was the use of semi-structured online interviews, which facilitated data collection. From the research, there was an in-depth comprehension of the issue of cyberwar and cyber-crimes. The Respondents were issued with surveys to explain the issues that affect the citizens in relation to Cybercrime and how this has impacted their livelihoods, finances, and day-to-day lives. The respondents explained government and non-government agencies' role in ensuring that cybercrime is thoroughly addressed and sustainable solutions are attained through the online surveys. The study participants helped in understanding the current state of Inter-agency coordination amongst all the relevant actors in finding a sustainable solution to the threat of cybercrime. They also expressed their opinions on the state and non-state actors in the fight against cybercrime, which may also elucidate more on the efficiency of the collaboration between the two agencies in the fight.

For this study, qualitative research was preferred over the quantitative method due to its multiple advantages. It was most suitable to help attain the objectives of the study. One of the key considerations that led to choosing this method of study was that it was more appropriate for small samples, where its outcomes are not quantifiable and measurable.[53] Another key reason behind settling for qualitative research over quantitative research is that it offers a thorough description and analysis of the research subject. It also does not limit the study's scope or the nature of the respondents' responses.[54] Nevertheless, the qualitative study's effectiveness is mainly based on the abilities and skills that a researcher has. There may also be the issue of reliability. In many cases, the outcomes are not considered reliable since they come from a researcher's interpretation and judgment.

For qualitative research, there is also a clear description, unlike quantitative research, where the aim is to classify and count features to explain what is observed.[55] The qualitative research is also subjective, where the event's individuals' interpretation is important, unlike the quantitative method, whose subject is to get precise measurement and analysis of the subject topic. Based on this study's nature, qualitative research also benefited from capturing the changing attitudes within the target group. This type of study also provides a much more flexible approach, where it was easy to quickly adapt questions, especially if useful insights were not getting captured.[56] It also helped in allowing for one to be more speculative about areas of investigations, leading to quality data, which can help meet the objectives of the study. This type of research was also more targeted, meaning that the most suitable person to be part of the study was selected,

[53] Connelly, Lynne M. "Trustworthiness in qualitative research." *Medsurg Nursing* 25, no. 6 (2016): 435-437.
[54] Aspers, Patrik, and Ugo Corte. "What is qualitative in qualitative research." *Qualitative Sociology* 42, no. 2 (2019): 139-160.
[55] Yates, Jennifer, and Tricia Leggett. "Qualitative research: An introduction." *Radiologic technology* 88, no. 2 (2016): 225-231.
[56] Ibid

which could help improve the quality of the research and ensure that the goals and objectives of the study are reached. This also helped in speeding the process of capturing data, and as a result, helped in keeping the costs of data gathering down.

1.8. 3 Study Site

In the online interview, the respondents also expressed their opinions on what should be done by the two actors in helping develop structures that will help fight cybercrimes that have been rampant in many countries, including in Kenya and Zambia. The respondents were also required to expound more on international collaborations in the fight against cybercrime. The collaborations amongst nations can help develop sustainable and effective solutions to the challenge of cybersecurity. The reason behind understanding international collaborations is based on the fact that there are multiple cases of persons committing cybercrimes across the globe, requiring all governments to work together to solve this challenge.

1.8.4 Target population

The selected sample members were individuals with prior knowledge on issues of cybercrime and cybersecurity. The respondents also had to have sufficient and relevant work experience in security or cybersecurity. They had a proven research background and understanding of the raw data concerning the topic of study. The study participants included six (6) persons from security agencies based in Kenya and Zambia and four professionals from Private companies involved in cybersecurity. All the participants had the characteristics and knowledge required to meet the study's objectives., They had the information required. Through theirviews, opinions, and recommendations, this study will analyze the findings and deduce the most suitable recommendations on how to deal with cyber threats faced in most countries.

1.8.5 Sampling frame/sample size

The sampling method used for this study was purposeful sampling, which is a non-probability sampling technique. The sample members were selected based on their knowledge and expertise on the subject of study.[57] The sampling considered both members of the government and private organizations who are conversant with the subject matter. The data collected from these ten (10) samples were adequate to provide meaningful results, which could help attain the study's goals and objectives. A sample of fifty (50) respondents was picked from government offices. Fifty questionnaires were administered across the Government Ministries, Departments and Agencies through the Heads of Information Communication Technology (ICT) departments or units. Interviews with the officials in government Ministry in charge of Information Communication Technology was held. The data once collected was analyzed and presented by use tables and graphs.

1.8.6 Data collection methods

The main data collection method was the use of primary sources, where online in-depth surveys and interviews were undertaken. The main aim of using this method was to identify the feelings, emotions, and opinions about this subject.[58] This is a method which entails systematic data gathering from a target audience. In this case, the method was characterized by sending an invitation to the selected participants. There was the use of a questionnaire in which the respondents replied to the asked questions. This was through their email addresses. After answering the questions, they would send the questionnaires back. This was a faster and more

[57] Sharma, Gaganpreet. "Pros and cons of different sampling techniques." *International journal of applied research* 3, no. 7 (2017): 749-752.

[58] Ball, Helen L. "Conducting online surveys." *Journal of Human Lactation* 35, no. 3 (2019): 413-417.

convenient way of data collection than undertaking a one-on-one interview.[59] First of all, it was an affordable method, since the costs of transport and other complex logistics were reduced. In the COVID era, there was also a need to ensure that physical contacts are minimized. Therefore, he online surveys served as the most suitable tool for the research.

Despite several drawbacks of this method, the data collection process acted as the most effective and could bear the most positive results, hence helping meet the study's goals and objectives.[60] The time span used to complete the online questionnaires was also relatively shorter, making the process faster. This was because the information was gathered automatically/real time without having to wait for the questionnaires to be returned. The margin of error of online surveys was also greatly reduced, where the participants had the option of entering their responses directly into the online system.[61] This was hence a better method than the traditional methods that rely on the attentiveness of a researcher to enter data correctly. In this method, there is a high likelihood of a human error.

By using this particular data collection method, the collected information was relatively easier to analyze. It was also easier for the participants to use, where all of them had access to the internet, and could hence answer the questions and then back as faster as possible. Most of the data collection process questions were semi-structured, where they also provided the researchers with the interview guide. Most of the questions were prepared to guide the research process and satisfy the research objectives. Additional questions were nevertheless made during the interview process. Some of the questions included in the semi-structured questionnaire include:

[59] Evans, Joel R., and Anil Mathur. "The value of online surveys: A look back and a look ahead." *Internet Research* (2018).

[60] Rice, Stephen, Scott R. Winter, Shawn Doherty, and Mattie Milner. "Advantages and disadvantages of using internet-based survey methods in aviation-related research." *Journal of Aviation Technology and Engineering* 7, no. 1 (2017): 5.

[61] Nayak, M. S. D. P., and K. A. Narayan. "Strengths and weakness of online surveys." *IOSR Journal of Humanities and Social Science* 24, no. 5 (2019): 31-38.

Question 1:	What is the current state of international Inter-agency coordination amongst all the relevant actors in finding a sustainable solution to the threat of cybercrime?
Question 2:	How can the state and non-state actors collaborate to fight against cybercrimes and ensure sustainable cybersecurity in their respective nations?
Question 3:	What is the current state of collaboration between government and non-state actors, and how effective is the collaboration in the fight against cybercrime?
Question 4:	What measures should be taken by the government and other non-state actors to ensure that there are constant structures in place to fight with the increasing cases of cybercrimes?
Question 5:	What are the different strategies that the Kenyan and Zambian state and non-state actors have to protect the institutions and the citizens in their respective countries?
Question 6:	Is there any international collaboration amongst these nations that can help develop effective cybersecurity solutions?

To complement the primary data, there was also the use of secondary sources. This entails the use of relevant textbooks, government publications, journal articles, commentaries, criticism, and histories, among other materials with information regarding the study's topic. The key reason for incorporating this particular research method was because they might have had complementary information that could not have been found in the primary data collected.[62] There are numerous sources with information regarding cybercrime and security, which were very important for this particular study, and hence had to be integrated into the study. Secondary data collection was also relatively quickest and with the least costs, where sources were collected from physical libraries and online platforms. They also help in providing a variety of expert insights and perspectives. To

[62] Tate, Judith Ann, and Mary Beth Happ. "Qualitative secondary analysis: A case exemplar." *Journal of Pediatric Health Care* 32, no. 3 (2018): 308-312.

ensure that the secondary data was quality and relevant to the subject topic, data collection was from peer reviews and scholarly articles, whose authors permit to use.[63] Secondary sources also help match the primary sources by addressing major issues that could not be achieved when collecting the participants' data.

1.8.7 Validity of data collection instruments

The only key instruments used were the online platforms through either phone or computers to answer the asked questions in the online survey. For confidentiality purposes, the raw data acquired from the interview was not shared with any third party.

1.8.8 Reliability of data collection instruments

The instruments are greatly reliable in that they enabled an accurate capturing of data and ensured that comprehensive information regarding the subject matter was acquired.

1.8.9 Data analysis and presentation

After data collection, there was a need to undertake a thorough qualitative analysis to evaluate the most suitable data for findings, conclusions, and recommendations on the issue of cybercrime. For this particular study, there was a content analysis of the data gathered from the online interviews. The collected data were categorized into themes and subthemes, which would enable easy comparison of the collected data. A key advantage of this type of analysis is that it helps the collected data be simplified and reduced, which can help produce quality results. Content analysis is also very vital for this particular research.[64] It enables a structure to have qualitative data collected, which greatly helps achieve the set research objectives. Nevertheless, using this

[63] Ibid

[64] Stalph, Florian. "Classifying Data Journalism: A content analysis of daily data-driven stories." *Journalism Practice* 12, no. 10 (2018): 1332-1350.

type of content analysis has several drawbacks, including the risk of researchers having a misinterpretation of data, leading to false and unreliable conclusions.

After evaluating the collected data, there was checking and editing, where the various deduced themes were grouped to have related units. This was followed by a comprehension of the presented themes in ensuring that it was easy to understand all the data collected. The interpretation would then be used as the facts. This was followed by the generalization, which entailed identifying the different interviews, which would allow for the development of typologies. The differences from the themes and sub-themes were then grouped into paragraphs. The last part of the analysis entailed the validity of the data, which would entail reading through the collected and evaluated data to ensure that the correct data would be noted down as the findings, which would help in the discussion for the study.

1.8.10 Ethical considerations

In every research, there is always a need to abide by the ethical guidelines. First, all the study participants were required to agree to voluntarily agree to participate in the study, without making any compromise. They were all sent an online link where they would agree to the study's terms and conditions. If one wishes to withdraw from the study, he/she was required to, without any compromise, state it with or without any reason. All the respondents were informed about what the study entailed its key objectives and any guidelines guiding the study.

Confidentiality is another key matter that was addressed in the course of the study. All participants were informed that no personal information would be shared with any third party. The information they would submit would be used only for academic purposes and for this particular study. Their personal information, such as names, email addresses, and any other personal information, would not be shared or used in any of the studies.[65] The research process was very comprehensive, where academic terms and technical words were used without any bodily or psychological harm to the respondents. A climate of comfort was created for the participants to ensure that they were comfortable answering the survey questions on the subject topic.

Ethical standards help ensure that there is the promotion of the truth and knowledge and that the primary goals and objectives are obtained. It also ensures that an environment of research, accountability, responsibility, and mutual respect are attained.

By handling the high ethical standards, the research was able to observe all integrity issues and, as a result, have quality data, which would help in the attainment of the study goals and objectives. Other codes of conduct observed in the study included non-discrimination, honesty, transparency, and social responsibility.[66] For the secondary sources, the ownership of online scholarly articles and books was acknowledged. The data used was also adequate, relevant, but not excessive, where its key aim was to complement the collected data. The study also ensured to use only authorized books and those up to date to ensure that the quality of the information is relevant to the current times.

1.8.11 Scope and limitations

As expected in any particular study, there are multiple limitations that may deter the progress of the research process. In this process, the first limitation was some unconfirmed or verifiable information from some of the respondents, which could not be used for the study's findings and discussions. Another major limitation is the complexity of the cybersecurity topic, which is constantly changing with time. There is a constant shift in the paradigm in which cyber-

[65] Clark-Kazak, Christina. "Developing ethical guidelines for research." *Forced Migration Review* 61 (2019): 12-13.
[66] Clark-Kazak, Christina. "Developing ethical guidelines for research" *Forced Migration Review* 61 (2019): 12-13.

criminals undertake their activities. This may limit some of the research findings in future, where there is likely to emerge new methods of committing crimes.

An additional key limitation identified in the research process was the conflicting information given by different parties, making it hard to have the best conclusion. This is because many participants gave their personal views and opinions, which sometimes could contravene each other or contradict information on the secondary source. Despite this situation, only verifiable information would be used for the study to ensure that only facts and provable information would be added.

Another key challenge identified from the study is that the research cannot be generalized due to the small sample used. Therefore, it may have failed to factor in other locations across the globe, where it generally majored in mostly Kenya's and Zambia's case studies. Another limitation is the fear of bias amongst the respondents in their answers. The participants of the study could, in some instances, have been biased in the way they answered the questions asked, more so on explaining about situations that the nations have been going through and also the state of collaboration between the state and non-state agencies in combating cybercrimes. A bigger sample could have probably enhanced the reliability of the study. Finally, due to the COVID 19 pandemic, it was impossible to undertake one-on-one interviews due to the fear of contracting or spreading the virus. This forced the study only to be undertaken through online platforms that may also have multiple disadvantages. Nevertheless, despite the limitations, the study was adequately undertaken, with a thorough analysis of all the points raised, to ensure that it could meet the set goals and objectives.

1.9 Chapter Outline

Chapter one entails the introduction of the research topic and highlights of what the study will entail from stating the background of the study, the problem statement, the Objectives of the Study, the Literature Review, Conceptual Frameworks and Methodology.

Chapter two involves an in-depth analysis and exploration to examine the current state of international, inter agency coordination amongst all the relevant actors in cybercrime prevention in both Kenya and Zambia.

Chapter three will involve the evaluation of measures taken by the government and other non-state actors to mitigate cybercrimes.

Chapter four will involve the critical analysis of the challenges faced both by the state and non-state actors in their collaboration in the fight against cybercrimes and ensuring sustainable cybersecurity policies.

Chapter five will involve the recommendations on the issues identified and a conclusion of the study.

CHAPTER TWO

ANALYSIS AND EXPLORATION TO EXAMINE THE CURRENT STATE OF INTERNATIONAL, INTER AGENCY COORDINATION AMONGST ALL THE RELEVANT ACTORS IN CYBERCRIME PREVENTION IN BOTH KENYA AND ZAMBIA.

2.1 Introduction

After undertaking a thorough research and reading former studies on the issue, from Chapter one, chapter two addresses and examines the current state of international, inter agency coordination amongst all the relevant actors in cybercrime prevention in both Kenya and Zambia. From the research it is manifest that, African nations have been greatly affected by cybercrime activities in the most recent times. The continent is among the fastest-growing regions in terms of cybercrime activities, where it is also a source of significant cyber-attacks that targets the rest of the world. This has necessitated for several measures to be undertaken to address cyber threats and improve cybersecurity in the continent. Two of the nations that have been affected by this challenge are Kenya and Zambia. The two nations through the interrelationship between state and non-state agencies have undertaken multiple measures to help with fighting the cyber threats. There have been multiple legislations that can help fight the crime, and also other enforcement measures. The efforts of the private sector have also been very vital in strengthening cybersecurity.

It is estimated that over a billion people in Africa will have access to the internet by 2022.[67] This, according to analysts, is likely to lead to an increased number of hacking activities. Cybercrime is shifting towards the emerging economies, where there is a growing number of

[67] SAMBULI, N., MAINA, J., & KAMAU, T. Mapping the Cyber Policy Landscape: Kenya. (2016): Retrieved from https://www.gp-digital.org/wp-content/uploads/2016/12/Kenya-Cyber-Policy-Mapping-final-i-1.pdf

cybercriminals. Many economies are hence becoming important sources, as well as the victims of cyber threats.[68] As a result of such threats, according to Kshetri (2019), Kenya, for example, incurred an annual loss of $210 million in 2017 alone as a result of the increased cases of cyber-crime. [69] There is hence a need to undertake a thorough insight and study in the increasing cyber victimization and threats in Africa, with the key aim being Kenya and Zambia. This will hence help in understanding the role of both state and non-state agencies in fighting the threat and addressing the increasing threat.

2.2 Fighting cybercrime in Kenya

2.2.1 Kenya state agencies involved in fighting cybercrime

The Kenyan government, the civil service, and other non-state actors have a great role in helping secure the country against cybercrime. A key body that helps in dealing with the issue of cybercrime is the ministry of Information Communication and Technology, whose mandate is to formulate, administer, manage and develop the Information, Broadcasting and Communication policy".[70] The ministry also has the role of regulating the information communication sector. It has most cases been responsible for formulating and implementing the ICT policy. It also develops and facilitates ICT infrastructure in the country. Some of its policy priority areas include capacity building in the ICT sector constantly having a review and amendment of a legal and regulatory framework.

[68] EUROPOL. 2011. The Changing Face of Cybercrime. https://www.europol.europa.eu/newsroom/news/changing-face-of-cybercrime.

[69] Ibid

[70] Kshetri, N. (April 2019). Cybercrime and Cybersecurity in Africa. https://doi.org/10.1080/1097198X.2019.1603527

The ministry of Information Communication and Technology is also responsible for the promotion of regional and international cooperation on matters to do with ICT.[71] It has also been mandated with the role of reviewing and updating the national ICT policy, which helps in the development of the ICT sector. The ministry is hence the leading body that deals with the issue of leading the state efforts in the fight against cybercrime and maintains cybersecurity. The Information and Communication Technology Authority (ICTA) was established in 2013, where its key mandate was to rationalize and streamline the ICT functions of the Kenyan government. The body deals with enforcing the ICT standards and also ensuring that there is comprehensive supervision of electronic communication. The authority is also mandated with promoting ICT literacy in the country, innovation, and capacity.[72] This means that it has a huge obligation to provide leadership with regard to cybersecurity management framework.

Communications Authority of Kenya (CA) is another key government body that is mandated with the role of facilitating the development of ICT sectors which include electronic commerce, telecommunications, and multimedia. On cybersecurity, it helps with providing cybersecurity sector regulations. The authority has held multiple conferences and meetings to develop the best ways of dealing with cyber insecurity in the country. According to the company website, there was a cybersecurity meeting, which called for the expedition of a data protection bill and investment in more professionals to help in curbing cybercrime in the country.[73] In a meeting conducted by the authority, a major issue faced by Kenya is the lack of cybersecurity skill sets, hence positing multiple threats to the government institutions, individuals, and businesses.

[71] Ibid

[72] Ibid

[73] Communication Authority of Kenya. 2019. *Cybersecurity meeting calls for expedition of Data Protection Bill and investments in more professionals.* https://ca.go.ke/cybersecurity-meeting-calls-for-expedition-of-data-protection-bill-and-investments-in-more-professionals/.

Lack of cybersecurity skill sets gives the criminals an easy way out, where it is hard to undertake cybercrime analysis, prevent, detect, and prosecute the criminals. According to the CA website, Kenya reportedly has between 16,000 and 17,000 cybercrime professionals in the country. [74]This is against 52 million mobile subscriptions, 49 million data subscriptions and 32 million registered mobile money users. The CA has been very vital in enhancing the security of the cyberspace of the country.

The government through the relevant authorities continues to operate the National Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC), which helps in the coordination and also, making responses to cyber threats. [75]The National KE-CIRT/CC also has the role of being the government's point of contact on matters to do with cybersecurity. The body in collaboration with other government stakeholders the private sector and the civil society. In terms of the Global cybersecurity Index, Kenya was ranked 2nd in Africa and 44th globally. The ratings are measured on its ability to capacity build, technical, organizational, legal, and cooperation. National KE-CIRT/CC was also established to offer advice on matters to do with cybersecurity, where it aids in coordinating cybersecurity. The body collaborates with local, regional, and global actors, to coordinate cyberspace and deal with cybersecurity. It also acts as a national trusted point, where it is contacted on matters of information security. National KE-CIRT/CC also helps in collecting, coiling, and disseminating national statistics on incidents that are related to cybersecurity. [76]It constantly undertakes a study on the development of computer security and helps identify the shifting paradigm on cybersecurity threats in the country.

[74] Ibid

[75] Ibid

[76]The National KE-CIRT/CC. 2012. *Cybersecurity: past, present and future.* https://www.ke-cirt.go.ke/index.php/cybersecurity-past-present-and-future/.

Other critical government actors in Kenya include the Kenya law reform, which has a statutory role of making reviews to the law of Kenya.[77] The body ensures that the laws are modernized and harmonized with the constitution of Kenya. The body has a huge mandate in ensuring that there is updating of legislation of cybercrime laws. Some of the cybercrime laws, which the body helped to formulate, include the Computer and Cybercrimes Bill, 2016, which helps in tackling the threat of cybercrimes in the country.

Another key institution in Kenya is the national intelligence services. This is a department within the ministry of interior. It has the mandate of identifying conditions that threaten the nation's economic, social and political stability. It works towards developing strategies and techniques of neutralizing the threats. The body helps in collecting intelligence, which can be very helpful in limiting the threat faced by the country, and more so cyber threats. The NIS works with other industry stakeholders, in ensuring that any type of threat, including cyber threat, is minimized. [78]NIS collaborates with Technology Service Providers of Kenya (TESPOK) and the ICT Authority in acquiring intelligence that will help in neutralizing threats. The body has a dedicated cybercrime unit that together with other industry players acts as a liaison. The National Police Service is also responsible for the fight against cybercrime. This is a body that helps in investigating cybercrimes through the office of the directorate of criminal investigations.

Other key government agencies in Kenya that help in combating cyber threats include the Office of the Director of Public Prosecutions. The office prosecutes criminal cases. They also have been very monumental in the enactment of the Kenya Cybercrime and Computer-related Crimes

[77] Ibid

[78] The National KE-CIRT/CC. 2012. *Cybersecurity: past, present and future.* https://www.ke-cirt.go.ke/index.php/cybersecurity-past-present-and-future/.

Bill of 2014.[79] All individuals accused of cybercrime are taken to court and prosecuted by the ODPP. Another key government body that helps in tackling cyber threats in the country is the Central Bank of Kenya. This is since it is very instrumental in shaping the fiscal policies in the financial sector. A key cyber threat in the country is in the financial sector, where it requires the leadership to engage CBK in the cyber policy landscape. A collaboration of the Central Bank of Kenya with other bodies greatly helps in detecting suspicious activities that are related to national cybersecurity. The central bank of Kenya has IT experts who ensure that security measures against cybercrime in the country are in place. The central bank also collaborates with the KE-CIRT/CC, where it is a member of the task force which was constituted to formulate the computer and cyber-Bill of 2016. [80]

2.2.2Non-state actors involved in fighting cybercrime in Kenya

The non-state actors play a crucial part in the war against cybercrime in the country. The government views civil society as a very key party in the policymaking process. This is since civil society helps in making critical contributions which help in ensuring that all areas affecting ICT and cybercrime are addressed. The civil society in the country has been very monumental in participating in the discussions, which led to the drafting and also passing of the national cybersecurity strategy. The civil society in collaboration with the state agencies has also constantly had an engagement session, where their say on the issue of ICT and cybersecurity help in the

[79]

National Cybesrsecurity Strategy. 2014. *Ministry of Information Communications and Technology.* http://icta.go.ke/pdf/NATIONAL CYBERSECURITY STRATEGY.pdf.

[80] The National KE-CIRT/CC. 2012. *Cybersecurity: past, present and future.* https://www.ke-cirt.go.ke/index.php/cybersecurity-past-present-and-future/.

identification of sustainable solutions. Some of the civil service organizations and non-governmental organizations that have been vocal and monumental in helping to draft policies and laws that help in averting cybercrime include Triple OKLaw Advocates, LLP, Telecommunications Service Providers of Kenya (TESPOK), Centre for Intellectual Property and Information Technology Law (CIPIT), Euclid Consultancy Services Limited and Hivos Regional Office East Africa (HIVOS ROEA), among many others. The private actors are important in the governance of cybercrime since this is a challenge that has been greatly affecting both the state and non-state institutions. The relationship between the two actors is very clear since each of them has their role to play in sharing ideas and in helping provide solutions that can help in averting the offenses.

The non-state actors help in conveying engagement sessions with civil society and different government entities on various issues in the ICT sector. They also help in the coordination of participation proceedings, where one of the proceeds includes the 2014 African Union Convention on Cybersecurity. The non-government bodies help in advocating and litigating for policies, where they also help in the capacity building programs. Many NGOs participated in the formulating of laws such as the 2014 Kenya cyber-Crime and computer-related crime Bill.[81] The Non-state actors in Kenya have also been very vital in sharing analysis with the government bodies and as a result help in influencing the policies. They ensure that all the set policies reach the human rights standards and that none of the enacted policies regarding cybercrimes are in place to cause oppression or affect the rights of the citizens in the country, hence promoting cyber security and

[81] National Cybesrsecurity Strategy. 2014. *Ministry of Information Communications and Technology.* http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf.

at the same time protecting the people in the country. A majority of the affiliated non-state actors have continually helped the government in addressing multiple challenges in the ICT sector and the technology stakeholders, where they are vital in guiding resolution mechanisms. Through their ideas, the bodies have helped in fostering development through the exchange of ideas amongst the industry stakeholders. It is therefore evident that both the state and non-state actors greatly work together to ensure that the challenge of cybercrime is addressed. Kenya has a long history of non-state actors providing social services where they have both collaborative and conflicting relationships in certain matters. On cybersecurity, most actors have been offering support, guidance, and direction on the best ways of approaching the matter.

Other non-state actors in Kenya who have been very vital in the implementation of cybersecurity acts include ICT professionals, journalists, and bloggers. This group was very vocal in the discussion of the Computer Misuse and Cybercrimes Act of 2017, when they shared their concerns about certain provisions. Some of the provisions they discussed according to them impinged on their constitutional rights and freedoms. They were mainly concerned about the inclusion of offences such as cyber-squatting and phishing, which they stated that they ought not to be have been a part of the Bill.

Following their intervention on the issue, the National Assembly of Kenya made a number of amendments to the Bill, where it considered the proposals aired by these non-state bodies and the public in general. As a result, the Computer Misuse and Cybercrimes Act was later passed and assented by the president as of May 2018.[82] Nevertheless, there is still a petition in the High court of Kenya that challenges the constitutionality and the legality of some of the provisions of the Act.

[82]SAMBULI, N., MAINA, J., & KAMAU, T. Mapping the Cyber Policy Landscape: Kenya. (2016): Retrieved from https://www.gp-digital.org/wp-content/uploads/2016/12/Kenya-Cyber-Policy-Mapping-final-i-1.pdf

[82] EUROPOL. 2011. The Changing Face of Cybercrime.

The amendments that were made to the Bill include the introduction of the National Computer and Cybercrimes Coordination Committee whose main goal is to advise and coordinate national security organs on issues related to computer and cybercrimes.

The committee is also mandated with coordinating the collection and analysis of security organs on issues related to cyber threats and responses to cyber incidences. The National Computer and Cybercrimes Coordination Committee was also tasked to receive and act on reports which are related to cyber-crimes and at the same time advise the national government on critical and emerging technologies such as block chain technology and mobile money. It would also help in the establishment of codes and frameworks that would be vital in the management of critical national information infrastructure. Finally, the committee had the mandate of training security personnel on the way of preventing, detecting, and mitigating computer and cybercrimes. This committee comprises of the Kenya Defense forces, the national intelligence service, the national police service, the ministry of interior, and representatives from the office of Director of public prosecutions and the Attorney General. Other additional members include the Central Bank and the Communications Authority of Kenya.

According to the amended bill introduced by the National Assembly on fighting computers and the cybercriminal offense, there were some additional offenses which brought about the controversy, with some non-state bodies and the civil society. The offenses included cybersquatting, which entails the unauthorized use and intentional use of a name, trademark, or domain name, owned or used by another person.[83] The second offense introduced in the amended act was phishing, which entails the creation of operating a site or sending a message with an

[83] Mwasaria, Mbatia. "Kenya: The Computer Misuse and Cybercrimes Act." *Update to article: 'Kenya: The Computer And Cybercrimes Bill of 2017'*, November 2018.

intention of inducing a person to disclose personal information, in which the penalty of this offense was a fine not exceeding three hundred thousand(300,000) shillings or imprisonment for a term not exceeding three years or both. Other new offenses introduced by the national assembly included the wrongful distribution of obscene or intimate images, identity theft or impersonation, failure by a worker in a given company to relinquish access codes, and also the failure to report cyber threats to the NCCCC.[84] Other offenses introduced by the parliament in this act included the interception of electronic messages or money transfers and cyber terrorism, which entails the access or facilitating access to a computer or computer system or network to commit a terror act.

Nevertheless, there has also been a conflictual relationship, where some of the non-state actors such as the Bloggers Association of Kenya ("BAKE") have been opposed to some cybercrime bills, which appear to be oppressive and belittling the rights of the citizens. An example is the Computer and Cyber Crime Act of May 2018, which was signed into law by the government. Some of the civil society bodies and non-state actors were against the act, where they were opposed to some parts of the section, such as the criminalizing in the publication of false information or hate speech. This is since it failed to explain what the bill entailed in this context. According to the opponents of such a bill, whose aim was on matters of cybersecurity,

such clauses would be used against citizens. BAKE’s main contention with the act is with the constitutionality of the standing orders of the national assembly, where it claims that the state body permitted the inclusion of some clauses into such Bills without the required public participation.[85] This led to a temporary suspension of twenty-six sections of the Act. Most of the suspended sections are related to computer and cybercrime offenses, where they include unauthorized interference, interception, the publication of false information, false publications, cyber

[84] Ibid

[85] Ibid

harassment, squatting, child pornography, impersonation, and identity theft, among others.[86] The issues are contentious, according to BAKE, since they are not comprehensive enough and well detailed for the public, hence could wrongly be used by the government bodies such as the police and the Prosecuting organs to wrongfully prosecute innocent citizens.

2.3 Inter-agency coordination in fighting cybercrime in Zambia

With the thriving cases of cybercrime in Zambia in the African continent, both the government and other non-state agencies have been keen on developing the most suitable measures that would help in combating the threats. Zambia has experienced an increased number of online fraudsters, which is attributed to the high number of internet users. On top of such threats, the country is also faced with other pressing issues such as poverty, financial instability, and also other traditional crimes such as rape, murder, and theft. This hence has led to it lagging in terms of fighting cybercrimes. There is also another challenge of lack of IT knowledge and the absence of suitable legal frameworks, which would help in dealing with cybercrime at local and national levels, hence compounding the problem in the country.

Zambia's case is almost similar to Kenya, where there is the coordination of state and non-state agencies, who help in fighting the crimes. The role of the government is key where the parliament of the country, together with other state agencies, help in enacting laws that can help fight the crime. In the country, cybercrime is relatively a new phenomenon in the business community. These are only a few institutions that play critical roles in combating

the crime. This is similar to many developing nations that have been experiencing increased cases of cybercrime. People and businesses have experienced huge sums of money getting electronically stolen from their accounts. Cyber-crime has also led to a disruption of businesses through

[86] Ibid

corrupting critical business systems by hackers. Social media is also getting highly misused in Zambia where there are cases of child pornography, invasion of privacy, theft of data, and many other cybercrime-related issues.

The parliament of Zambia has nevertheless taken lead to ensure that there are laws that target cybercrime. The parliament in 2004 passed the Computer Crime and Misuse Act No. 13, which is a law that criminalizes cybercrimes such as hacking, service attacks, and unauthorized access and modification of data.[87] A major challenge that has affected the country since then is the increased utilization of ICT, which has increased the number of cybercriminals. As of 2016, the number of internet users rose to 3,167,934, which is 20.4% of the Zambian population, according to IWS. Currently, the penetration rate of internet users is 6.1 million, which represents 39%. Many people are keeping pace with technological developments, where they have computers and smart devices which as a result has led to an increased number of criminals that use the devices. Despite the existence of the Computer Crime and Misuse Act No. 13 of 2004, no person in Zambia has been prosecuted under this act. The country had a launch of the National ICT policy and the Seventh National Development Plan, which calls for assessing if the government commitment to addressing cybersecurity concerns.

The need to have specific cybercrime laws in Zambia was contributed by the case where a young Zambian hacked into the website of the statehouse, where he replaced the photo of President Fredrick Chiluba with an image of a cartoon. She was arrested and charged for defaming the Head of State, which was contrary to the Section 67 of the penal code.[88] The court nevertheless failed to

[87] The Parliament of Zambia. 2004. *The Zambia Computer Misuse and crimes Act, 2004.* https://ictpolicyafrica.org/en/document/0vodshuq3cj?page=4&raw=true.

[88] https://www.news24.com/news24/zambia-to-delete-cyber-crime-20040729

continue due to lack of a law which dealt with cybercrime in Zambia. This hence forced parliament to enact laws that could help in the prosecution of such criminals.

The minister of communication and transport introduced the computer Misuse and Crimes bill. The key objectives of the bill were to prevent abusive use of competitive system`s, prohibit unauthorized access or interference by the use of a computer. The bill also sought to protect the integrity of the computer systems and ensuring that there are confidentiality and integrity of data. Another aim of the bill was to help in the facilitation of gathering and using an electronic device to commit cybercrimes.

Both the government and non-state agencies of Zambia have been very crucial in creating awareness to the consumers on matters of cybercrime. This is through having educative programs, sensitizing on the need for being secure and holding forums that involve the public. The country, through the government, introduced the National Policy Framework on Cyber Crime. This is intended to criminalize the cybersecurity, activities, and misuse of computers. The government approved a global cybersecurity protocol intended to protect internet users in the country. Nevertheless, the government has been criticized for lacking equipment, skills, and organizational abilities, which could help in fighting cyber-crime.

The government of Zambia, in 2006, through the ministry of Communication and Transport came up with a formula for National information and Communication Technology Policy. This policy recognized that the world has embraced information and communication technology as an enabler of social and economic development. The policy also recognized that ICT was very vital in the contribution of global trade and investment. The policy by the government was set to ensure that Zambia participates in the global economy. As a result, it helped the government in promoting information and knowledge-based society as the basis for creating wealth. Despite the setbacks, the policy was critical in ensuring that many private firms adopted the use of technology. There is a significant lack of physical and logical protection for the ICT infrastructure, where there is a growing number of cyber-attacks in Zambia as technology continues to advance.

Currently, the government of Zambia is undertaking numerous efforts to help in minimizing the cases of cyber threats, which continue to increase. The effects of cybercrimes in the country have affected the national economy, making the government develop more plans, where together with the non-state agencies continue to come up with the best measures of tackling the challenges. Policy frameworks in the country have helped in encouraging communities, individuals and organizations, to invest in information and communication. There is however more urgency for analyzing the national ICT policy, as a way of addressing concerns that regard the deterrence of using ICT in criminalizing activities that involve computer technology. The National ICT policy of 2007 was enacted to coordinate all matters of ICT in the country. The goals of the policy are to ensure that there is further use of ICT in the country. The government acknowledges that ICT also offers an opportunity for criminals to commit acts with ease and with little risk of apprehension.[89] This has as result demanded evaluation by the government of Zambia to have a commitment to more policies, which would help deal with culprits.

A key goal of the national policy is to “Develop the Legal & Regulatory Framework” and “Promote Security in the Information Society”. This policy desires to develop an appropriate institutional, legal, and regulatory system that supports the development of a competitive national

[89] Hanyama, Nchimunya, and Dani Banda. 2017. *Policies and Legislation for Internet Access and Usage in Zambia.* http://article.sapub.org/10.5923.j.scit.20170703.02.html.

ICT sector. This is to be supported by a fair and transparent legal and regulatory framework. To attain these goals, the government has made various commitments. First, the Zambian government aims at putting in place effective laws by the parliament to adhere to national, regional, and international standards.

The government of Zambia has also ensured to implement effective laws and regulations which will help in combating cybercrime at national, regional, and ultimately at the international levels. It also has the role of addressing the national ICT policy, which helps in the promotion of practicing professionals in the ICT industry. This move is key in ensuring that there are competent men and women, who are willing to make contributions that will make the country's cyberspace safer for all the country’s citizens. The Information Communication Technology Society of Zambia is in charge of setting standards for ICT personnel in the country. Unfortunately, up to now, the body does not have the power of regulating the training of ICT professionals, to register or discipline them.

The government of Zambia has embarked on a mission, where it intends to establish a computer crime investigation unity, which will help in the enforcement of cyber law and also help in the National electronic communication security center.[90] Once these bodies are actualized, then they will be under the strict supervision of internal organs that are specialized security agencies. This move will be advantageous to the country in that it will help in eliminating the establishment of independent units, which have proven to be too costly and time-consuming during establishment. The government together with other relevant stakeholders on a

Computer crime investigation unit will be a positive move and supported at all costs in that currently the country lacks great expertise in the enforcement of its cyber laws. Through

[90] Ibid

enactments of more laws, the government with the help of the parliament will ensure that there are policies that would help in the prevention, detection, and promotion of the response to cybercrime and misuse of ICT. This can help in combating the major crimes in the country, which include fraud, money laundering, terrorism, pornography, etc. at the national, regional, and global levels.

Another vital body that is a part of the government of Zambia is the National Electronic Communication Security Centre. It helps with complementing the forts safeguarding the ICT infrastructure networks and systems.[91] This is a body within the government that is likely to help in the process of reforms, by ensuring that there is an activity, authenticity, and integrity, and confidentiality of the government. The two bodies working together in Zambia are also mandated with ensuring that there is consumer privacy, data, and information content integrity and also addresses security concerns that are triggered to damaging and corruption the cultural heritage, national image, and identity of Zambia.

The Zambian Opposition has over time expressed concerns on the intended proposals by the government to introduce tough new cybercrime laws, where it states that this could be to clamp down social media rather than prevent the threats of cybercrime.[92] This was after the government tried to introduce three bills, which were designed to promote the responsible use of digital platforms. According to the government of Zambia, on the contrary, through the introduction of such bills, its only intention is to protect the Zambians who for a long time have been victims of internet scams and also hate speech. The three bills introduced in the Zambian parliament included

[91] Chisenga, Sydney. April, 2020. *Zambia - Data Protection Overview.* https://www.dataguidance.com/notes/zambia-data-protection-overview.

[92] CHAWE, MICHAEL. 2018. *Zambia opposition MPs reject move to introduce new cyber laws.* https://www.theeastafrican.co.ke/tea/rest-of-africa/zambia-opposition-mps-reject-move-to-introduce-new-cyber-laws-1397652.

the cybersecurity and cyber-crime act, the data protection act, and the electronic transactions and electronic commerce act[93]. The Acts had an intention of promoting responsible use of digital platforms and also safeguard the users of electronic platforms that included social media from dealing with unscrupulous users, who would have a key aim of harming them. The legislative body in Zambia has a key mandate of legislating bills that can help in dealing with such threats of cybercrimes.

The ICT regulating body in the country is also very vital in that together with the legislation, they can work together in developing cybercrime legislation. Regulators in the country possess s experience in matters of data protection, the confidentiality of data transmissions and also are vital in the prevention of spreading of malicious software. Their expertise can therefore be very important in helping the legislatures adopt effective bills and acts that can help prevent cases of cyber threats in the country. The regulatory body in Zambia is also conversant with the criminal laws, which are known to violations of obligations in the traditional areas of regulatory work, and can use ion maters of dealing with cyber threats. The regulatory body in the country is also vital in the implementation of laws in that it plays an advisory role in the development of strategies that the country can undertake as a way of dealing with the crimes, and developing sustainable solutions for combating such criminal acts.

The communication Authority of Zambia was also very monumental in helping to daft the cybercrime-related legislation, namely the Electronic Communications and Transactions Act 2009.[94] This was through sharing ideas and solutions with the other government bodies and the legislature, where the act helped in solving several cyber-related threats affecting the country. The

[93] Ibid

[94] ICT Policy Africa. 2009. *The Electronic Communications and Transactions Act, 2009.* https://ictpolicyafrica.org/en/document/fujb45s0qsb?page=3.

evidence of Zambians performance in the utilization of ICT can be founded in various indices of international organizations. For example, according to the 2017 E-Government Development Index, which was published by the United Nations Department of Economic and Social Affairs, Zambia ranks 132 out of 193 in utilizing ICT. According to the International Telecommunications Union in its 2015 ICT Development Index, Zambia ranks 153 out of the 167 countries that participated in the research. This is clear evidence of the low ranking of the country in the utilization of ICT, which also reflects on its preparedness in dealing with matters involving cybersecurity and threats. The ranking of Zambia in these indices is also an indication of the need for having accelerated ICT development as a way of effective and efficient supporting the economic recovery mad preparedness of the country as a whole through the coordination of both state and non-state agencies.

According to the minister of Transport and communication of Zambia, the country is in the process of establishing a cybersecurity institute, intending to prevent cyber-attacks, more so as the country is making efforts to digitize its economy. Further, the Zambian government in conjunction with key non-state agencies is in the process of developing firewalls in cyberspace which will help in detecting possible cybercrimes. According to the government representatives in the country, Zambia is getting more and more vulnerable, such as other African nations, meaning that it ought to put more effort to ensure that it effectively and thoroughly fights against the threat of cyber threats. The government is in the process of establishing more cybersecurity strategies since most of the businesses and activities both within the government and in other private institutions are gradually adopting the use of modern technology, which is internet-based and poses more threats of cyberattacks.

It is nevertheless evident that Zambia still lacks enough legal framework and strong infrastructure which can help in dealing with cybercrimes in the country. In the country, just like in the case of other developing nations, proper coordination between the top-level government officials, policymakers, and other non-state agencies, where such coordination would be vital in the establishment of structures and legal frameworks that can help deal with the growing threat of cybercrimes in the country.

2.4 International coordination

As a Way of enhancing the fight against cybercrimes, both Kenya and Zambia have had to coordinate with international agencies that are relevant to the issues of such crimes. Kenya together with its counterpart East African nations has scaled its efforts to combat emerging cases of cyber-crimes, through undertaking a multi-stakeholder approach. The approach involves the governments, industry, and civil society groups. The coordinated activities amongst the regional counterparts are aimed at rooting out cyber threats among the five East African community members.[95] There is a task by the member states who deal with the cybersecurity policy, legal and regulatory levels. The five-member states include Kenya, Uganda, Tanzania, Rwanda, and Burundi, with South Sudan, being the latest member to join. The EAC members have set up Computer Emergency Response Teams (CERTs), which are mandated with helping in fighting the threats, where they involve the International Telecommunications Union's (ITU) for assistance pertaining to the issues. The member states also have an umbrella body which is The East African Communications Organizations (EACO) Congress that pursues the ITU support to establish the national CERTS.[96] The EACO has the role of establishing and harmonizing internet security

[95] Quarshie, Henry Osborn, and Alexander Martin-Odoom. 2012. "Fighting Cybercrime in Africa." 2(6): 98-100. doi: 10.5923/j.computer.20120206.03.
[96] Ibid

policies and also enacting internet laws that would give the East African region. The body has also adopted proposals for the telecommunications operators, which is needed to form and run the sectoral CERTS, and also nominate representatives from each of the member states.

Zambia, together with other SADC member states have acknowledged the fact that unless they give much focus to the creation of the requisite harmonizer policy environments, then they mail fail to realize the full potential of ICT and also fail to develop both legal and regulatory frameworks, which will help in the promotion of ICT diffusion and use. In collaboration with other SADC members, there has been a development of a SADC model legislative provision and guidelines which deal with pertinent ICT issues, as a way of clearly defining the digital landscape. Nevertheless, this, model legislative provision fails to specifically address matters concerning cybercrime, hence failing to find sustainable solutions to this emerging threat. The collaboration with other member states such as SADC members is very vital for the establishment of solutions to the threat of cybercrimes. This is since, through such coordination, cyber freedom which is a serious global challenge can be thoroughly addressed, where sustainable solutions to the challenge can be identified and implemented through relevant bodies.

Through regional partnerships, both Kenya and Zambia have managed to discover multiple sustainable solutions that could help in introducing cyber legislations that would help minimize the number of cyber threats affecting them. An overarching East Africa’s policy guideline on cybercrimes is the African Union’s Convention on Cyber Security and Personal Data Protection. The policy was adopted by African Union member states in 2014, in a convention similar to Europe’s Cyber Crime Convention that was also established to deal with the issue of Cyberthreats in Europe. [97]This is a convention that requires the member states to share responsibility by undertaking certain cyber security measures that consider the correlation between cybercrime and data protection. The convention is also very vital for the African nations since it encourages the establishment of national computer emergency response teams.

From the convention, dual criminality was created as a provision, where suspects of cybercrimes can be tried in the country where the crime was committed or in their home country. This is in order to encourage smooth cooperation between member states without any conflict of laws. From the convention, there was a provision of mutual legal assistance, where member states can allow shared intelligence and also collaborate in undertaking investigations. Despite Kenya, not being a signatory, it has undertaken legal and policy frameworks adopted from the convention.[98]

International coordination with other global bodies and governments has also been very vital in the fight against cyber threats which is a common global phenomenon. Among the international bodies that both countries work to deal with cyber threats include the United Nation on Drugs and Crime (UNODC), Council of Europe (CoE), Us Department of Homeland security, Microsoft Corporation, and the World Bank, among other global bodies. Through international coordination, it is relatively easier for countries to exchange intelligence on matters involving cybercrimes and threats across the globe.[99] The international community has been on the front in enhancing national law enforcement capabilities and also help in the facilitation of international

[97] The conversation. December 2019. "What's been done to fight cybercrime in East Africa." https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240.

[98] Ibid

[99] Quarshie, Henry Osborn, and Alexander Martin-Odoom. 2012. "Fighting Cybercrime in Africa." 2(6): 98-100. doi: 10.5923/j.computer.20120206.03.

cooperation on cybercrime. Other leading agencies include the Interpol's Global Cybercrime Program and Innovation Centre in Singapore, Europol's European Cybercrime Center, and the Joint Cybercrime Action Taskforce.[100] All international agencies are in support of corporation between the public and the private sectors as a way of intensifying efforts to fight the threats. Interpol has over years been very vital in collaborating with local security organs to detect, avert and also make arrests on persons involved in crimes across the globe, were through excellent coordination, great strides towards dealing with the threats of cybercrime. Through international coordination, relevant authorities can get important intelligence regarding cyber-related crimes across the globe. The coordination also greatly helps in soliciting necessary funding that can help the fight against cyber-related crimes across the globe.

2.5 Conclusion

From the cases of both Kenya and Zambia, it is apparent that both the state and non-state actors are very vital in ensuring that they develop the most effective strategies that can help in combating cyber threats affecting the countries. Failure by the two bodies to coordinate effectively means that there may be multiple gaps on matters of legislation and implementation of effective strategies leading to increased cases of cyber threats to both the government bodies, private institutions, and innocent citizens. It is also apparent that Cybercrime and cybersecurity are two issues that can hardly be separated, where the issue of cyber threat has been a growing challenge to governments and nations, hence needing to be thoroughly addressed by the relevant bodies, which are from both the government and non-government parties.

[100] Stock, Jürgen, Michael Daniel, and Tal Goldstein. 2020. "Partnerships are our best weapon in the fight against cybercrime. Here's why." https://www.weforum.org/agenda/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/.

From the case of Kenya, it is apparent that the national assembly had to involve other government and non-government stakeholders in participating in the development and enactment of cybersecurity bills that would help tackle the issues related to the threats. Despite the dispute of the 2017 Bills, major clauses were upheld by both the agencies and as a result enacted by the parliament. Through such bills, it is relatively easier for the security organs to identify, arrest, and prosecute cybercriminals easily and as result minimize the cases of threats in the country. Such bills, help in enhancing cybersecurity and protection of critical information infrastructures, which help in ensuring that there are national security and economic wellbeing. Through the involvement of multiple agencies solutions that make the internet safer, are also identified, hence ensuring that the growing number of internet users in the country are protected and are safe to make any engagements and transactions through the use of the internet.

Similarly, to Kenya, Zambia experienced an increased number of cyber threats. This has as result, lead to a need for more coordination between the government and other non-state bodies, to identify multiple suitable solutions that would help combat the rising cases of threats. Nevertheless, the country has relatively fewer institutions that could help in tackling the crime. One of the most crucial body has been the Parliament in conjunction with the ministry of information, who have been vital in the enactment of the cyber-crime acts and bills that help in combating cyber-related crimes. The non-state agencies in the country have also played a vital role in the legislation of bills, by providing insightful recommendations and analysis of the matters to the parliament and other bodies. Nevertheless, the major critic of the bills enacted has been the opposition in the parliament who are concerned with some of the clauses enacted by the parliament. They view them as an infringement of the rights of the ordinary citizens.

Collaboration with international bodies such as INTERPOL and the World Bank has been very monumental in the fight against cybercrimes. The nations, in collaboration with such bodies, can have in-depth information regarding cybercrime development across the globe, and as result develop new measures that can help in averting or dealing with such threats. International coordination also enables nations to easily exchange intelligence on matters involving cybercrimes and threats across the globe. The international community has been on the front in enhancing national law enforcement capabilities and in facilitating international cooperation on cybercrime. Nevertheless, it is evident that in both the case of Kenya and Zambia, there is a need to have more international and interagency coordination as a way of having more sustainable measures to deal with the fast-growing threat of cybercrime in the African continent.

CHAPTER THREE

AN EVALUATION OF THE MEASURES TAKEN BY THE GOVERNMENT AND OTHER NON-STATE ACTORS TO MITIGATE CYBERCRIMES

3.1 Introduction

Chapter two systematically provided an in-depth analysis and exploration to examine the current state of international, inter agency coordination amongst all the relevant actors in cybercrime prevention in both Kenya and Zambia. For this chapter an in-depth evaluation of measures taken by the two government and other non-state actors to mitigate cybercrimes. Both the government and the non-government actors have been very monumental in the fight against cybercrime. Their role has been crucial given that cyber threat has brought with it several new threats that ought to be comprehensively addressed. Cyber dependency has become a widespread social activity, with complex interconnections between different sectors, and hence has increased vulnerability to attacks against both civilian and military infrastructure. There hence has been an increased focus on cyber defense within the armed forces and also by the national security organizations in many parts of the globe, including Kenya and Zambia. For the military, for example, cyberspace has been identified as a new fifth arena, besides land, air, water and space in which military operations can be performed.[101] Some of the measures undertaken by the government include an increased focus on cyber offensive and defensive measures, which are performed both independently and as a complement to conventional warfare.

Nations globally are also concerned about the economic and human rights benefits and disadvantages as a result of the global connectivity. China, for example, according to Singer and Friedman, (2014) is developing its network of firms behind the great firewall, where it is planning to allow for screening of incoming messages and if needed disconnect from the worldwide internet[102] according to an article from Yale law school. All of these trends have emerged as a result of the internet "converging into a perfect storm that threatens traditional Internet values of openness, collaboration, innovation, limited governance, and the free exchange of ideas." Some of the issues that are a result of the internet will have consequences beyond the internet, where there

[101] Sigholm, Johan. "Non-state actors in cyberspace operations." *Journal of Military Studies* 4, no. 1 (2013): 1-37.

[102] Singer, P. W., & Friedman, A. 2014. Cybersecurity And Cyberwar What Everyone Needs To Know. Oxford University Press.

is a growing vulnerability in the physical world from the new vectors of a cyber-attack through the virtual world. In the future, the wars will not just be about soldiers, who use guns and jets, but rather will be through the use of the internet, where there may be weaponized computer programs that disrupt or even destroy critical industries such as transportation, communication, utilities, and energy.[103] Cybercrime could be used to also disable military networks, control how troops move, control the path of jet fighters, and also control warships. This depicts the effects of the internet and how it could change the nature of war and conflicts about nations or communities.

As a result, countries are greatly investing in cybersecurity to ensure that they are prepared in the event of any cyber-attacks, which could have numerous harms on their operations and may put their citizens at high-risks in the event of an attack.[104] The fears of such attacks are leading to the militarization of cyberspace. Such visions of future wars through cyberattacks deliver massive amounts of information, innovation, and prosperity to the wider planet, where they fuel tensions between nations. This is a matter of concern, which means that both government and non-government agencies in countries need to be thorough in getting innovative and research on how to incorporate cybersecurity structures that address the importance of cybersecurity, as a way of securing institutions and the citizens.

3.2 Government interventions in the cybercrime war

There has been an increased government intervention on matters concerning cybersecurity and also partnerships and collaborations with other non-state actors as a way of ensuring that the

[103] Singer, P. W., & Friedman, A. (2014). Cybersecurity And Cyberwar What Everyone Needs To Know . Oxford University Press.

[104]Sigholm, Johan. 2016. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies.* doi:https://doi.org/10.1515/jms-2016-0184.

challenge finds sustainable solutions. Governments including the governments of Kenya and Zambia have had collaborations with civil society organizations and the private sector, where they have continually developed strategic measures of curbing the threat of cybercrime within their specific countries.[105] Many governments across the globe have provided visions and strategies that help in incorporating sustainability in public policy, which help in transitioning their specific economies based on sustainability principles.

The main role of the government is to take care of its citizens, their businesses, and livelihoods and to protect them against harm. A government can hence improve the environmental performance of firms by ensuring that it has measures in place that curb the rising cases of cybercrime. This is through having advanced innovations in all sectors of the society since this will lead to changes in the sector and also ensure that more sustainable measures are introduced. There is hence a rising need for technology and policy innovation, in the fight against cybercrime. The traditional role of the government has been to protect public interests and also regulate industries.[106] This role of the government is gradually changing, where presently the governments are closely working collaboratively with other stakeholders from private entities such as the civil society, in ensuring that sustainable measures are in place, which will ultimately help in protecting the people, business, and institutions.[107] The responsibility of the governments is also changing, where the whole future of a sustainable world is getting shaped by policy decisions made by the governments individually or in collective forums.

[105] Young, S. T., and K. K. Dhanda. "Chapter 9: Role of governments and nongovernmental organizations." *Sustainability: Essentials for Business; SAGE Publications, Inc.: Thousand Oaks, CA, USA* (2013).
[106] Ibid
[107] Ibid

The cost of cybercrime to the global economy is estimated to rise to 500 billion dollars per year according to experts.[108] This is an issue that took the center stage at the World Economic Forum Day, which prompts governments across the globe to undertake stringent measures that can help protect the companies of these specific nations. From the event, it was apparent that cybersecurity was the third biggest global risk just behind extreme weather events and natural disasters. This shows the need for government to manage the tasks, and ensure that solutions that can help curb the threats are in place.[109] It also illustrates the rapid pace of the challenge, which has been on the rise as a result of the increased digital economy. The cybercrime challenge falls alongside the growing industrialization of the global cybercrime industry resulting in one of the most pressing and pervasive challenges facing business and wider society today. According to WEF's global risks, cyber breaches recorded by businesses have doubled in five years, from 68% in 2012 to around 130% by 2017. Cybersecurity is quite a complex issue because of the dynamic nature of the evolving threat landscape that requires firms to constantly review and evolve their strategy on cybersecurity, procedures, and policies. Most organizations in African countries are hence equipping their staff members with the necessary skills and awareness that help firms to boost their defense, as a way of combating the ongoing challenge. Given the high threats of cyber threats across the globe, there has been some good progress concerning the public-private sector collaboration, as a way of tackling the challenge head-on.

[108] Ismail, Nick. 29 January, 2018. "Collaboration is key in fighting cybercrime." https://www.information-age.com/collaboration-key-fighting-cybercrime-123470569/.

[109] Ibid

The government, for example of Kenya, is already proactively reaching out to organizations that are conversant with matters of cybercrime or those that have been affected by cyber events as a way of sharing knowledge, expertise and also offer the necessary support. Collaboration with private entities has helped in collaborating, assessing, and distributing the threat intelligence from the industry and the government sources, hence helping in curbing the rates of crimes.[110]A key organization that governments across the globe have been collaborating with intending to curb the cases of cybercrime include Interpol, which is vital in providing intelligence on cases of cyber threats and also providing information that can help in identifying and taking actions against cybercriminals.

There have been both local and international laws that seek to address the issue of cyberwar. There are well known and widely accepted principles of cybersecurity. Nevertheless, applying them to cyberattacks has been a challenging task for a challenging task. This difficulty arises out of the fact that the law of war developed, for the most part, in response to conventional wars between states. When there is a cyber-attack in progress, it is hard for the state to evaluate the scope of an attack or figure out the person responsible for the attack. Such difficulties have made nations reluctant in responding to attacks in defense for the fear that they may be violating the law of war. [111] The growing importance of cyberspace to modern society is increasingly becoming an arena for major attacks, and as a result, has become a major security concern for

[110]Ismail, Nick. 29 January, 2018. "Collaboration is key in fighting cybercrime." https://www.information-age.com/collaboration-key-fighting-cybercrime-123470569/.

[111]Tan, Aaron. 2017. "Collaboration is key to combating cyber crime." https://www.computerweekly.com/news/450421906/Collaboration-is-key-to-combating-cyber-crime.

governments and armed forces internationally. The major unique characteristics of cyberspace that make it a growing concern and challenge to governments include its low cost of entry, its symmetric nature, the lack of attribution, and the ambiguity associated with it.[112] Another key characteristic of cyberspace is its role of acting as a medium for crime, espionage, and military aggression, which as result has made it a domain for state and also non-state actors in cyber conflict.[113] According to the global nature of cybercrimes, then it means that no nation or firm can solely fight it on its capabilities. To address the challenge, there ought to be a collaboration between various stakeholders. According to Interpol, this is vital in that it will help address the challenge of transnational and organized crimes. Governments have the role of sharing information regarding cyber threats. This is to ensure that there is speedy and efficient communication, which helps in easily catching up with the cybercriminals. Collaboration and sharing of information have been proven to be vital in that multiple sources, credible reports, and any likely indispensable information that can help combat any cases of cybercrime will greatly help in reducing the type of harm that could have resulted in major losses for a country or institutions.

3.3 Measures undertaken as a result of the collaboration efforts between the state and non-state actors

In recent years, many nations have reported large scale cyber-attacks against their military defense systems, financial systems, and other critical infrastructure. Presently, there are no agreed-upon universal rules or norms which can help in governing the international conflicts in cyberspace.[114] Many governments opt to keep it that way, where they believe that there are

[112] Ibid

[113] Ibid

[114] Eilstrup-Sangiovanni, M. (2018). Why the World Needs an International Cyberwar Convention. *Philos. Technol*, 31, 379–407. doi:https://doi.org/10.1007/s13347-017-0271-5

numerous challenges in the verifiability and issues that are posed by the rapid technological changes. They hence rule out certain agreements on an international cyber convention. Governments in different nations prefer to rely on informal cooperation and strategic deterrence to limit direct conflict. There have been numerous reports of scores of attempted cyber-attacks on critical infrastructure to nations such as air traffic control systems, national electricity grids, satellite systems, and government structures. [115]The attacks on government systems have led to governments stressing the need for stronger cyber defenses, as a way of protecting the governments and institutions from the attacks.

Across the globe, multiple governments trace a range of views on how close the link between the state and non-state actors such as private companies should be. They also have different views on how to involve the non-state actors on matters of cybercrime. These differences amongst government have a profound influence on the culture of cyberspace as it develops. The relationship between the government and non-state actors makes sure that domestic attitude on issues such as national interest, intellectual property rights, and fair competition, which are prominent in shaping the cyberculture. [116]A balance between controlling cyberspace and having freedom in using cyberspace is hence a much-needed component.

Another important community with a key role to play in cybercrime prevention is the academic community, which will help in undertaking thorough research and development of the most suitable measures. Globalization has greatly played a role in the growth of cyber threats. The scale of the internet has been on growth, hence leading to the facilitation of organized crimes. This requires centralized coordination of intelligence amongst nations and non-state actors who will

[115]London Institute of Banking & Finance. 2017. "The changing face of Cybercrime." *A special report by The London Institute of Banking & Finance.* https://www.libf.ac.uk/docs/default-source/default-document-library/the-changing-face-of-cybercrime464f2e43ec86691782d0ff00001f97d9.pdf?sfvrsn=53c9478d_0.

[116] Ibid

ensure that resources are effectively utilized to help in the fight against cyber-attacks. The creation of awareness on individual and corporate user responsibility is another key issue that both state and non-state actors need to consider as a way of combating cybercrime.[117] The creation of awareness helps parties in identifying potential points of contact including illegal downloading, social engineering risks to the children, and securing if wireless internet connections.

The cyber-attacks threats have forced nations to be very keen on securing their networks and control the harm brought about by the Attacks. Despite numerous efforts undertaken by nations, more steps need to be undertaken as a way of enhancing the overall security of the national networks.[118] This is since; the current efforts undertaken are yet to enough, hence exposing the nations to more attacks. There have also been several legislative fights over cyber bills. Nations such as the US have been left exposed to a growing variety of cyber threats, hence leading to more need for cyber legislation. According to the London Institute of Banking & Finance (2017), cyber breaches are projected to cost the global economy $2.1 trillion by 2019, which was more than quadruple of the 2015 costs.

3.4 Efforts by the government of Kenya in combating cybercrime

The government of Kenya has been very instrumental in the fight against the rising cases of cyber threats. First, the government has undertaken campaigns, where it challenges businesses and corporations to develop and have measures that can help them to curtail the emerging cyber threats. According to the ICT Cabinet Secretary Joe Mucheru, the cyberattacks are real emanating as a result of high unemployment rates in the country, more so among the tech-savvy youth and

[117] Ibid

[118] Tan, Aaron. 2017. "Collaboration is key to combating cyber crime." https://www.computerweekly.com/news/450421906/Collaboration-is-key-to-combating-cyber-crime.

also a result of policy gaps in the country.[119] There is also an increased malware which includes ransomware, which could be attributed to weak cybersecurity measures, enforcement gaps, and standards within the firms. A major growing gap is growing in cybersecurity skills, which the government, together with the private sector has been working collaboratively to address.[120] Speaking at the launch of TAI Security Operations Centre an initiative by Strathmore University, ACPM Ltd based in Hungary, and BCK Kenya, the cabinet secretary empathized on the importance of collaboration between both state and non-state actors, where he commended such collaborations for the current strides made at curbing the threats of cybercrimes in the country and the region.

Centers such as the TAI Security Operations Centre, according to the CS, are important in that they offer real-time monitoring and advanced contextual analysis, which help in the prevention, detecting, and addressing security threats for the local Kenyan businesses. Such centers are emerging intending to respond to a massive increase of cybercrime cases across the country and region. [121]This is since, for example between January 2020 and June 2020, according to The National Kenya Computer Incident Response Team and Coordination Centre there were around 48.5 million cyber-attacks detected in the country. [122]

The Kenyan Government has been involved in the country's fights against cybercrime where it has introduced various policies and legal frameworks. One of the key frameworks is the

[119] OBURA, FREDRICK. November 8th 2020. "Kenya steps up fight against cybercrime." https://www.standardmedia.co.ke/business/sci-tech/article/2001393164/kenya-steps-up-fight-against-cybercrime.

[120] Ibid

[121] OBURA, FREDRICK. November 8th 2020. "Kenya steps up fight against cybercrime." https://www.standardmedia.co.ke/business/sci-tech/article/2001393164/kenya-steps-up-fight-against-cybercrime.

[122] Ibid

National Cyber Security Master Plan'. The framework recognizes that there is an increase in the use of technology by most Kenyans, a factor that has led to more frequent and dangerous cyber threats in the country. According to the data in place, there are over 13.1 million users of internet subscribers in the country, a figure that depicts the growing number of people that have access to the internet.[123] A former Cabinet secretary of Kenya's Information, Communications, and Technology (ICT), Dr, Fred Matiang'i stated that in 2013 alone Kenya lost over $2billion about $23 million) in 2013.[124] As a result, the ministry had no choice but to invite stakeholders to give their ideas, course of action and recommendations on what ought to be done to help in developing an action plan for cybersecurity strategy.

Among one of the solutions offered by Kenya's Ministry of ICT is assigning each person in the country with a virtual identity, as a way of curbing the rising tide. According to the former Information permanent secretary, Bitange Ndemo, the country was planning to establish a key public infrastructure, which will help in allocating virtual identities to the internet and also to digital service users. According to the PS, the procurement was already complete and the project was moving towards the implementation phase. According to the PS, the need for such measures was to ensure that citizens are protected against persons with evil intentions, who use the internet to commit cyber frauds to innocent civilians and institutions. According to the Ps, there was also a need for constant reviewing of policies and legislations, which would be to help the country keep pace with the evolving technology.

Protecting the county against cyberattacks, according to the Permanent secretary, would demand that the government is committed to developing comprehensive and offensive cyber

[123] Eweniyi, Odunayo. 2014. "Kenyan Government Joins the Fight Against Cybercrime." https://techcabal.com/2014/05/07/kenyan-government-joins-fight-cybercrime/.

[124] Ibid

capabilities, which would ensure that the threats and attacks are curbed. This is only achievable by hardening ICT infrastructures and services. There would also be a need to enhance ICT security competencies, where there would be increased international collaborations to make the security situation more resilient. The Government of Kenya has tried to make efforts that would create an environment of trust in Kenya's cybersecurity, through having a multiagency approach in the national cybersecurity management and also in having a child line protection.

One of the major strides by the government is through the development of the earlier mentioned Computer and Cyber-crime Bill 2016', which is one of the legislative frameworks of sealing loopholes used by cyber fraudsters to perpetrate offenses in the country. [125]The actualization of the bill was vital in that it helped in the development of laws that help in the prosecution of cybercrime offenders and also help in nationwide sensitization programs of cybersecurity among the law enforcers, prosecutors, and judicial officers. The government of Kenya is also in the process of developing an ecosystem of cybersecurity. This is in addition to having a research team, which has been constituted by the Communication Commission of Kenya (CCK).[126] The team has been created to help in the development of a cyber-crime counter-strategy. As a result, Kenya has been used as an incubator for teaching services like applications. This shows the efforts that the country has been undertaking to remain cybercrime secure.[127] According to the CS of IT, cybercriminals have continued to destroy or steal bank records, registries, and cash,

[125]Korir, Cheruiyot. November 29, 2016. "Government to curb cyber crimes." https://ict.go.ke/government-to-curb-cyber-crimes/.

[126] Ibid

[127]Business Daily Africa. NOVEMBER 19, 2012. "Kenya steps up fight against cyber crime." https://www.businessdailyafrica.com/bd/corporate/companies/kenya-steps-up-fight-against-cyber-crime-2019556.

despite the measures in place, hence meaning that the government will be required to continue developing further measures that will help curb the crime.

3.5 Conventions and conferences and their role in fighting cyber crime

There have been multiple conventions and conferences in the country and in the East African region, where the issue of cybersecurity has been adequately addressed. An example is the East African cybersecurity convention in 2012, which was aimed at bringing together both the government and the private sector players in Information Technology. Other parties in the convention included people in the security departments and various businesses across the region. The key aim of such a convention was to look for a common front in the fight against cybercrime, which according to IT security services company McAfee, increased by 43 percent in the third quarter globally and now tops $2.5 billion (Sh210 billion) in revenues. In the convention organized by Cyber Security Africa, the cyber threat was identified to be one of the hugest challenges to the security of organizations within the region. Cyber Security Africa, which is organizing the conference, says cyber threats have been identified as the most pressing challenge to the security of organizations in the region. According to Sammy Kioko, the manager of Cyber Security Africa alliance manager, rogue individuals, terror groups, and stateless organizations, can commit a cyber-attack from anywhere through the use of "a few strokes of the keyboard.[128] This has hence resulted in a need by both the government and the private sector to come together and have an active engagement in pursuit of the best measures of curbing such occurrences. Private entities such as the Huawei Broader way Forum, McAfee, SmoothTel, Sabric, Cloud Security Alliance, TESPOK, 3G, Academy Group, for example, in partnership with the ministry of information and communications came together to have in-depth dialogues on the most suitable measures and the

[128] Ibid

shifting paradigm in the fight against cybercrime in the region.[129] This is a clear indication of the importance of collaboration of state and non-state actors in the fight against such threats.

3.6 The private sector role

The private sector players who are mostly involved with the fight against cyber threats are those with an understanding of corporate and international dimensions of the threats. Others include the high-tech industries, renowned research universities, and institutions of higher learning, and also the public policy leaders who have knowledge and expertise in the field of cybersecurity. [130] According to McAfee account manager for East Africa, Emmanuel Kimeu, a company that was one of the sponsors of the convention, cyber warfare has gone, where institutions such as the United Nations have had a summit of dealing with it.[131] This is because the crime strategies have been changing over time, where mobile devices such as Android and iPhones, have been a huge target, making each individual or company very susceptible to the attacks. Another clear target of cybercriminals is digital transactions, hence making both the government and the private sector wary of the threat, hence developing a strategy countering the cyber-crimes. The plans involve securing the digital transactions and content and encourage investments in internet infrastructure to incorporate tougher security measures of dealing with the growing threats.

The government of Kenya has continually come up with more measures, which involve enhancing partnerships with the private sector as a way of boosting security to the digital economy.

[129] Ibid

[130] Business Daily Africa. NOVEMBER 19, 2012. "Kenya steps up fight against cyber crime." https://www.businessdailyafrica.com/bd/corporate/companies/kenya-steps-up-fight-against-cyber-crime-2019556.

[131] Ibid

According to the current CS at the Ministry of Information Communication and Technology, the private sector is very vital in that it has the expertise and the know-how of developing innovations that could enhance the security of the country's cyberspace. According to the CS, the government of Kenya is greatly committed to giving priority to collaborations on cybersecurity, with the private sector, where this can help in boosting the growth of the eCommerce sector and also help in the adoption of e-government services.[132] According to him, some of the most vulnerable institutions to cybercrime threats are the financial and health sectors, due to the type of sensitive data they deal with. Another measure taken by the Kenyan Government is enactment of more laws, which help in enhancing penalties for online crimes.[133] As mentioned in the previous chapters, there are multiple laws that the Kenyan parliaments in collaboration with non-state actors have ratified to help in the fight against cyber threats. Such laws have helped in ensuring that the threats are minimized and that the perpetrators are punished accordingly., This provide both short and long-term solutions to the challenge.

The high internet penetration in Kenya has also forced the government to make cybersecurity a national priority. This is as a result of a huge population depending on the digital platforms in delivering both private and public services. According to the IT CS, as much as the large corporations have managed to put measures in place to deals with cyberattacks, small firms are continually facing safety challenges. This is due to their limited experience in dealing with such magnitudes of threat, and also due to the huge resources required in the fight against the

[132] Xinhua. 2020. "Kenya to partner with private sector to boost cyber seurity." http://www.xinhuanet.com/english/2020-11/06/c_139496641.htm.

[133] Ibid

cyber-crimes. [134] Another emerging factor that the government ought to deal with is the COVID-19 pandemic, which has increased the vulnerability of the nation to cyber threats. This is because many people are likely to work from home using the internet space, due to the social distance guidelines.[135] The current nature of the cyber-crime, overall, means that Kenya and even developed nations are yet to be adequately prepared in the fight against cyber threats.

There have been other multiple initiatives that have been launched in Kenya, Zambia, and other countries in the continent to help improve the cybersecurity landscape. The most important of these is improving regulatory quality. According to a report by the African Union Commission (AUC) and the cybersecurity firm Symantec in November 2016, most of the countries have specific laws, which help in dealing with cybercrime and electronic evidence. Kenya's new Data Protection Bill has many elements of Europe's General Data Protection Regulation (GDPR). It for instance requires organizations to inform users on why their data is getting collected, the purposes of the data, and how long the firm would store the data. According to the bill, the consumers have the right to request firms to delete their data. Firms also are required to have certain levels of security standards when storing data, to help protect the consumers from privacy invasion. The bill is designed in a way that it can help citizens to have their data protected, a factor that can help in reducing cybercrime in the country.

Many governments in Africa, including Kenya and Zambia have also ensured that there are sector-specific regulations. This is because banking and other financial institutions, for example, are the most affected sector by cybercrime. For example, the bank of Ghana issued a

[134] Xinhua. 2020. "Kenya to partner with private sector to boost cyber seurity." http://www.xinhuanet.com/english/2020-11/06/c_139496641.htm.

[135] Ibid

Cyber Security Directive for Financial Institutions that required the involvement of senior executives and the board to have measures of strengthening cybersecurity. The banks in that country are required to appoint a Cyber and Information Security Officer (CISO), whose mandate would be to advise the senior management and the board on issues related to cybersecurity. He/she would be required to help in the formulation of adequate measures that manage cyber and information security risks. The same case applied to The Central Bank of Nigeria (CBN), where it announced that it was developing a risk-based cybersecurity framework for the country's financial institutions. Similarly, for Kenya, the Central bank in August 2018, asked any payment service providers to submit their cybersecurity policies to the government, to evaluate the measures they undertake to fight and prevent cases of cybercrime. Kenya, just like many African economies has also strengthened its enforcement measures.

The private sector cybersecurity in the country has been more prominent. For example, in early 2017, there was a Cyber Immersion Centre in Nairobi, established by Seraianu. This center is vital in the fight since it helps in providing an environment for the firms to experiment and test their cybersecurity capabilities. [136] The center also provides educational facilities, which help in the development of cybersecurity professionals. There are also more collaborations with multinationals, who have worked with local firms to help the consumers comprehend what cybercrime entails and assist in the development of ethical standards.[137] Multinationals such as Microsoft and Google have partnered with local firms to help in educating, and also developing measures that help fight cybercrime and create economic opportunities.

[136] Gercke, Marco, Tatiana Tropina, and Christine Sund. 2010. "THE ROLE OF ICT REGULATION IN ADDRESSING OFFENSES IN CYBERSPACE."

[137] Ibid

3.7 Mitigation efforts against cybercrime in Zambia

Although the Republic of Zambia has not experienced a physical terrorist attack, its government reaffirms its endeavor to continue its commitment to the principles set by the UN Security Council in regards to promoting international peace and cooperation among states. Its commitment is also influenced by the increased use of the internet and digital technology in the 21st century that has made it easy for terrorists to carry out their attacks.[138] The state remains cognizant of the different activities related to cyber terrorism and has therefore introduced different countermeasures in case of a future occurrence or threat. Through its government, Zambia has established different policies and agencies as well as collaborated with other non-state actors to fight cyber terrorism activities. The government is currently in a process of establishing a Center against Terrorism (CAT). This national agency which will include different national stakeholders will work collaboratively to create sustainable counter-terrorism measures. The body will also be responsible for the coordination of Zambia's security agencies such as the Police service and the Anti-Terrorism unit. CAT is established in response to the UN Global Counter-Terrorism Strategy that necessities the use of a multi-agency approach as a most effective way of responding to terrorism.

The Zambian government has started the process of amending the 2007 Anti-Terrorism Act to make it more effective. The Act was created to prevent any potential act of terrorism whether physically or through cyberspace, recommend mechanisms for detecting, and provide any relevant information to the law enforcement agencies. It will also codify CAT establishment as part of the wider counter-terrorism strategy. Additionally, Zambia is a member state of the Eastern and

[138] Ajayi, E. "Challenges to enforcement of cyber-crimes laws." *Journal of Internet and Information* 6, no. 1 (August 2016): 1-12.

Southern Africa Anti-Money Laundering Group that works collectively to implement the Financial Action Task Force regarding financing of terrorism activities and money laundering.[139] The task force is concerned with the control of financial flows that are associated with malicious activities. In collaboration with this task force, the Zambian government has operationalized the Financial Intelligence Centre (FIC). This multiagency body will monitor and control all financial systems including coordinating with other states to detect suspicious financial transactions. FIC which falls under the Ministry of Finance is supervised by the Central Bank and other Intelligence and Law Enforcement Agencies. FIC's responsibilities include receiving, initiating requests, and disseminating any relevant financial information to the relevant law enforcement agencies.[140] The body comprises of personnel equipped with the needed knowledge to detect and identify any suspicious financial transactions that may be related to money laundering or terrorist financing.

The government also introduced an anti-cybercrime law to help in the fight against cybercrime and cyber terrorism. The need for anti-cyber-crime law was influenced by an incident that involved a young Zambian who hacked into the statehouse website and replaced the president’s portrait with a cartoon image. Although the young Zambian was arrested for defaming the head of state, the case was dropped due to the lack of proper laws that dealt with cybercrimes in the country. During his arrest, the country lacked concrete laws that could guide the sentencing of cyber-related criminal activities. This incident necessitated the need to introduce cyber-crime laws that would prevent or mitigate cyber-crimes including terrorist activities. In 2004, the national assembly approved the Computer Misuse and Crimes Act to deal with cyber-terrorism

[139] Nanyun, Nankpan, Nasiri, and Alireza. "Role of FATF on financial systems of countries: successes and challenges." *Journal of Money Laundering Control* 1 (August 2020).

[140] Nchimunya, Hanyama, and Dani Banda. "Policies and Legislation for Internet Access and Usage in Zambia." *Science and Technology* (Scientific Academic Publishing) 7, no. 3 (2017): 72-78.

activities.[141]The law criminalizes activities such as hacking, unauthorized access or modification of information as well as denial of service attacks. Any individual found guilty of these activities is liable for a penalty which could be a fine or jail term depending on the severity of the situation. The law has continuously been amended to strengthen it and make it more effective especially during an era of rapidly changing technology inventions.

In 2006, the Zambian government through the Ministry of Communication and Transport introduced the National Information and Communication Technology Policy. The motive for the policy creation was the fact that Information and Communication Technology continues to evolve at a rapid pace and has become an important aspect of the global trade and investment sector. The policy considers the fact that ICT has become a critical subject among the UN MDGs and the World Summit on the Information Security (WSIS).[142] The policy further considers the fact that the rise in ICT has resulted in increased cyber-terrorist threats not only for Zambia but for the whole globe. The National Electronic Communication Security Center is another vital agency that further complements the efforts put in place to deal with ICT in particular cyber terrorism activities. The body works collectively with other institutions to ensure that public and private communication networks and systems are monitored as necessary, data integrity is enforced, consumers of the internet are well protected from terrorist and crime threats, and that the security of the state is not compromised by cybercriminals. The government has ensured that officers working in these institutions have the needed equipment to facilitate training and also effective management and control of security across the cyberspace. The National ICT policy has also been

[141]Kshetri, N. "Cybercrime and Cybersecurity in Sub-Saharan African Economies. In: Cybercrime and Cybersecurity in the Global South." In *International Political Economy*, 152-170. London: Palgrave Macmillan, 2013.
[142]Gercke, Marco. *UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE.* Telecommunications Development Sector, ITU, 2013, 1-366.

strengthened to ensure that security agencies are well coordinated and that security concerns can easily be identified and dealt with.[143]

In April 2018, a Cybersecurity and Cybercrime Draft bill was established to control communication over the internet and detect suspicious terrorism activities. The bill was established to detect fake news, cyberbullying activities, and other internet-based messages that appeared to threaten the national security. In particular, any individual found to have committed any of these offenses can be punished with up to one year in prison as well as penalized or fined.[144]The bill was established to work collectively with other established bills and policies to ensure cybersecurity in the country.

Different non-state actors have collaborated with government institutions to ensure that this policy achieves its mandate effectively. They include Zambia Information and Communications Technology Authority (ZICTA), Home Affairs Research and Information Development (HARID), and many others that work collectively to curb and mitigate cyber-terrorist activities.[145] Some of their responsibilities include conducting assorted research related to detecting and mitigating cybercrime activities, regulating ICT, and explaining laws about cyber-crime and terrorism activities. The government also works with international organizations such as the UN to fight cyber terrorism. For instance, a support portal dubbed' Victims of Terrorism Support' was established to show solidarity with the victims of terrorism. The portal is designed to show support and solidarity to those who have either been attacked, injured, or traumatized

[143] Nchimunya, Hanyama, and Dani Banda. "Policies and Legislation for Internet Access and Usage in Zambia." *Science and Technology* (Scientific Academic Publishing) 7, no. 3 (2017): 72-78.
[144] Nir, Kshteri. "Cybercrime and Cybersecurity in Africa." *Journal of Global Information Technology Management* 22, no. 2 (April 2019): 77-81.
[145] Nchimunya, Hanyama, and Dani Banda. "Policies and Legislation for Internet Access and Usage in Zambia." *Science and Technology* (Scientific Academic Publishing) 7, no. 3 (2017): 72-78.

because of terrorist attacks.[146] Being a member of the UN implies that Zambia is among the states whose population has greatly benefitted from this portal.

3.8 ICT regulators

Traditionally, the ICT regulators were not assigned any significant role to address the threats of cybercrimes. Instead, this role was mainly allocated to the domain of lawmakers and law enforcement agencies. However, in the current times, with the increasing ubiquity and openness of ICT networks, the ICT sector has become more vulnerable, hence requiring the inclusivity of ICT regulators to help with the fight. The vulnerability has been on a rise, to the increasing concerns of harmful and offensive content, and also due to the innumerable threats to critical infrastructure, and also to the integrity of computer systems and networks. Cyber regulators, both in Kenya and Zambia are very vital in that they help to reduce the questions of threats and the harm of individual users, businesses, and financial institutions. ICT regulators are mandated with facilitating the mobilization of different stakeholders and also help in coordinating efforts of these stakeholders in the fight against cyber threats. The long-term sustainability of the ICT industry in the continent and hence greatly depends on the regulators.

3.9 Role of law enforcement in curbing cybercrime

The security forces, led by the police, both in Zambia and Kenya have the role of maintaining public order, by detecting, monitoring, and preventing crime. As a part of the government, the police have the responsibility of ensuring that they unearthed any cybercrimes, and develops sustainable measures of fighting such crimes. Through their investigative efforts,

[146] United Nations. "Government Support: Zambia." *UN: Victims of Terrorism Support Portal.* 2020. https://www.un.org/victimsofterrorism/en.

more funding from the government, and engaging in more research, then the police force can help in dealing with the increasing number of cyber-related activities, hence protecting both public and private institutions and organizations. [147]In the past, the police have undertaken several raids on several cyber-related criminals, where they have been successful in arresting many cybercriminals. Despite their efforts, it is apparent that they have to put more effort and resources, to develop more sustainable solutions to the emerging global challenge.

Some of the existing approaches that are used by law enforcers to fight crime in the real world often do not work in cyberspace. Alternatively, they are inapplicable when dealing with issues that deal with ICT. This means that the law enforcers have the responsibility of having a comprehensive approach addressing various aspects of cybercrimes. There is a need for a shift in the current approaches used by law enforcers, which should be in line with the unique challenges that are new for legislators as well as the investigatory bodies. They must all take into consideration the paradigm shift in the IT sector and cybercrimes, to effectively fight crime in the virtual world.

According to a report by Tropina, there is a need for new skills that investigate crimes in cyberspace.[148] Government, through the legislature, has the role of reviewing the policing concepts that are in line with the changing needs in society. In the implementation of the policies, there will also be a need to ensure that the government agencies consider the shifting paradigm and environment, hence a need for continuous improvement. Some of the features to be considered by

[147]Tropina, Tatiana. 2009. "Cyber-policing: the role of the police in fighting cybercrime." *European Police Science and Research Bulletin · Special Conference Issue Nr. 2.* Germany.

[148]Tropina, Tatiana. 2009. "Cyber-policing: the role of the police in fighting cybercrime." *European Police Science and Research Bulletin · Special Conference Issue Nr. 2.* Germany.

the policing and investigative bodies include accreditation standards for advanced skills in cyber training, focusing on the national reporting system, and also having the outsourcing capability for forensic activities.[149] These tools are very critical in analyzing and finding sustainable solutions to the challenge of cybercrimes. The government, through the relevant agencies, has the role of developing mechanisms of the utilization of these tools and preparedness for participation in global mechanisms of cooperation on the national level.

Policing and investigating agencies globally can exchange critical information regarding cybercrimes and illegal online activities, which can help countries in investigating individual cases. The relationships amongst these agencies are very critical in that it ensures that there is the capacity necessary to conduct the investigations hence getting successful in the conquest of cybersecurity. [150] Nevertheless, apart from assisting the police in investigations, capacity building, and information sharing, the partnerships can also be directed towards the development of strategic partnerships with the non-state agencies and the ICT industry at large.

Most of the existing approaches to fighting crime cannot be applied in fighting cybercrime. This is because they are not applicable for efficient use in understanding ICT related criminal activities. There are various challenges associated with addressing different aspects of cybercrime, which also applies to the legislators and the investigatory bodies, who have to keep up with the shifting paradigm in fighting crime in a virtual world. The Internet has spread across the globe, both in developed and developing nations, where people use it in various businesses. It is used

[149] Ibid

[150] Jakobi, A.P, and K.D Wolf. 2013. "Non-State Actors All Around: The Governance of Cybercrime." *The Transnational Governance of Violence and Crime. Governance and Limited Statehood* (Palgrave Macmillan). doi:https://doi.org/10.1057/9781137334428_7.

mostly as a way of doing business, where it has become a driver of dramatic growth in the number of users in recent years.

As a result of the increasing number of people using the internet, then there has been a huge challenge for policing cyberspace. This is because, first, of the weak points that present an opportunity to criminals, where there is a clear lack of understanding of individual security online. Another challenge is mainly related to social engineering techniques. Another point of weakness is that while identity theft, spam, and phishing activities can be done automatically, without having to invest much effort or money.

Internet was designed as a network where people have open aces to information. This openness gives criminals an advantage, where they can easily find a tool or information that can help them commit crimes online. There is also easy availability of software and devices, which allow hackers to access password protection, easily undertake automated attacks, have robots for illegal purposes, and use search engines easily.[151] As a result, this has easily enabled people to use the internet for the wrong reason where they easily attack people or organizations or access information. Some of the information online entails instructions on how to commit the crime online, hence facilitating the development of crime both in cyberspace in the real world.

3.10 Role of the international agencies

Interpol is a key body on matters of fighting cybercrime. This means that the partnership with the body can help the police and investigative bodies of a country easily pursue cybercriminals and also protect local organizations and institutions against attacks. Some of the

[151] EUROPOL. 2011. *The Changing Face of Cybercrime.* https://www.europol.europa.eu/newsroom/news/changing-face-of-cybercrime.

initiatives of Interpol concerning cybersecurity include undertaking online investigations, computer forensics, public-private partnerships, training, review, and evaluation of technology, and also help in law enforcement. Interpol operates within the regional and international levels with other key security agencies to ensure that it can detect and unearth cybercriminals across the world, who mostly use the internet to either fraud, cause harm or hack security systems of institutions, organizations, and even individuals.[152] Interpol has over the years facilitated the sharing of information within participants. Interpol is an agency whose key mandate includes the functioning of a global 24/7 network that represents an early warning system between IT crime investigations units in various nations. It aims to facilitate operational contacts between Interpol National Central Reference Points (NCRP) for computer-related crimes.

Interpol also has the Child Abuse Image Database, which it maintains and runs. The database facilities assist in sharing of information and images which assist law enforcement agencies across the globe to identify victims and offenders. The agency has image recognition software, which helps in the comparison of details of where and how the abuse took place, and help o in rescuing the victims. The need for the database is since there have been increased cases of child sex abuse online, where the victims are forced into undertaking sexual acts, where they are posted on online platforms, which is against the law.[153] The database has helped Interpol, together with other law enforcers around the world to investigate arrest and prosecute many sex offenders, mostly after coordination of Interpol and the police in various countries.

[152] Wall, David S., and Matthew L. Williams. "Policing cybercrime: networked and social media technologies and the challenges for policing." (2013): 409-412.
[153] Ibid

3.11 Future partnerships in the fight against cybercrime

One of the most promising future policies in the fight against cybercrime cyberspace is public and private partnerships. This is because the private sector actors have played a very domain role in driving the ICT sector development and innovation. They also possess the infrastructure and have direct access to it hence making them vital players in the role of fighting cybercrime.[154]On the other hand, the government has the power of establishing legal orders and enforcing them through the police and other law enforcement agencies.[155] This means that collaboration between the two sectors could be very vital in the fight against cybercrime, where each will have very important contributions that can help make the process efficient, faster, and more successful. The two parties mutually complement each other and can help in the creation of the ground for voluntary cooperation.

When there is cooperation between the government and the private sector, both parties are also easily able to have a better understanding of the issues of addressing and preventing cybercrime. This is since neither of them can fight cybercrime alone, and will need each other's efforts, facilities, and resources to have effective responses to this emerging challenge.[156] Law enforcers greatly need the private sector, more so in the expertise on complex ICT issues, since in most cases they lack the knowledge in this field, especially in comparison with ICT sector experts. They also lack the capability and resources of monitoring all volumes of suspicious internet communication or even collect and record suspicious data, which can help in preventing crime.

[154]Jakobi, Anja P. 2013. "Non-State Actors All Around: The Governance of Cybercrime." 129-148. doi:https://doi.org/10.1057/9781137334428_7.

[155] Ibid

[156] Lovet, G. (2009) Fighting Cybercrime: Technical, Juridical and ethical Challenges, Virus Bulletin Conference, September 2009. available at: http://www.fortiguard.com/papers/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf

This depicts that criminal justice and successful investigations of a crime depends on the great extent of the ICT industry, and also on the internet service providers.

It is also apparent that despite the ability of the private sector to be resourceful with facilities and skills, it will also require the government to help it in several hurdles.[157] Despite the power and the size of a private corporation, it would still need the government to help it with investigations, legislation, and the prosecution of offenders. The government has the power to enact laws through the legislations, to undertake investigations through investigative agencies, and also to arrest and prosecute the offenders, which the private sectors have no mandate to undertake.

3.12 Conclusion

Despite the many advantages associated with the growth of modern technology and the use of the internet, the downside of the development has been the rise of cyber insecurity. Most developing and developed nations across Africa, and globally have been faced with the threat of cybercrimes. This has been mostly contributed by the growing number of internet and modern technology users in the world. Kenya and Zambia have as a result over the years been forced to undertake multiple measures of combating the threat that has been facing government institutions, private organizations, and also individual citizens.

One of the most effective measures has been the enactment of laws and regulations which help in combating, regulating, and minimizing the threats faced as a result of cybercrimes. Another major measure undertaken by the two governments is empowering their respective security organs and other critical stakeholders to ensure that they are fully skilled with the right tools that can help

[157] Tropina, Tatiana. 2009. "Cyber-policing: the role of the police in fighting cybercrime." *European Police Science and Research Bulletin · Special Conference Issue Nr. 2.* Germany.

combat the threats. Collaboration with non-state actors such as private financial institutions and other parties with deep knowledge about the threat of cybercrime and matters involving cybersecurity has also been one of the key measures of helping the government deal with the threats. Other measures undertaken by the respective government and non-state actors involve holding conventions and conferences, where stakeholders and experts in cyber security discuss the best way forward in the future that would ensure that the citizens and institutions are safe and are well equipped in dealing with future threats, which have posed huge threats.

Collaborating with international bodies such as Interpol is also another effective measure that has largely helped in providing intelligence on cases of cyber threats and also providing information that can help in identifying and taking actions against cybercriminals. Nevertheless, despite all the measures undertaken, there is undoubtedly a need to have more effective actions. This is because cyber threats are on a rise due to the increasing number of people using the internet, and the ability of cybercriminals to develop more innovative ideas and tactics. There is a need for adopting more measures and strategies by the government, private bodies, and relevant international agencies, to help in keeping up with the modern technology and outdoing the cybercriminals now and in the future.

CHAPTER FOUR

ANALYZIS OF THE CHALLENGES FACED BOTH BY THE STATE AND NON-STATE ACTORS IN THE FIGHT AGAINST CYBERCRIMES AND ENSURING SUSTAINABLE CYBERSECURITY POLICIES

4.1 Introduction

From chapter three, it is apparent that cyber-crime is the new trend of theft and crime in the world. Every year, cyber criminals earn trillions of dollars illegally. Businesses, individuals, and public institutions have all been affected by the events of cybercrime., Both the state and non-state actors across the globe have been making major efforts intending to deal with this rapidly growing type of crime. Nevertheless, in their fight against this digital crime wave, there have been multiple challenges and obstacles that prevent these actors from attuning sustainable solutions to the issue.

4.2 Reasons why Cyber-crime remains to be a major challenge

A major reason why it has been very hard to fight cyber threats is that criminals can analyze/scan a situation. There has been an evolution of cybercrime, wherein in the early 90s the malware was pushed out by the use of floppy disks before the emergence of the internet. Then as the internet and email became common, the criminals invented better methods of infecting machines and systems. An example of the most infamous malware was the "*ILoveYou*" virus. [158] In 2017, there was the emergence of cryptocurrencies, which gained popularity, and the bitcoins hit very high values. As a result, cybercriminals were able to develop specialist malware with the name of crypto mining bots, where the malware would turn a computer into a slave with an intention of mining cryptocurrency. After the Bitcoin dropped, the criminals dropped to explore

[158] Sprinkel, Shannon C. "Global Internet Regulation: The Residual Effects of the ILoveYou Computer Virus and the Draft Convention on Cyber-Crime." *Suffolk Transnat'l L. Rev.* 25 (2001): 491.

other fields, which they could easily steal from individuals and organizations. The examples are evidence of how challenging it is for agencies to get to them or end these crimes since they are continually evolving. The internet has given the cybercriminals an environment in which they can easily evolve, and also up their game over the relevant authorities and agencies.[159] Malware and phishing continue to increase, allowing the novice to enter into the world of cybercrime. The evolution of criminals is major threats and challenge to the agencies, both in and outside the government.

Another major reason why cybercrime remains to be a challenge is social engineering. Cybercriminals are very manipulative and are easily able to learn human behavior. Social engineering involves tricking a person into doing their bidding. Phishing fraudsters fit a particular crime to the situation easily, where when the situation changes, then they change their tactics. Most of the global data breaches have been a result of social engineering. One of the most common ones is spear phishing, where individuals are closely targeted and their credentials of the system administrators are easily stolen.[160] A case of such a cybercrime was the Uber company systems were breached. Another key reason why Cyber Crime has continued to become a major challenge to nations is the ability of cybercriminals to quickly and rapidly change malware.[161] Many of them are bright and conversant with the systems, where they have created malware that easily adjusts to the environment it ends up in. [162] An example is the banking trojan, which can easily adjust if it gets repackaged, to avoid detection by the antivirus software. This is referred to as Polymorphic malware, making it one of the most challenging malware packages to detect or prevent. The fireless

[159] Lee, Laura. "Cybercrime has evolved: it's time cyber security did too." *Computer Fraud & Security* 2019, no. 6 (2019): 8-11.

[160] Button, Mark, and Cassandra Cross. *Cyber frauds, scams and their victims*. Taylor & Francis, 2017.

[161] Luknar, Ivana M. "Cybercrime-Emerging Issue." *Archibald Reiss Days* 10 (2020).

[162] Ibid

malware is getting more popular by data, since it can go for months with getting detecting, and in the process, it gets to steal data including log-in credentials, where cybercriminals, then get records or undertake other criminals' activities such as emptying individual or company accounts. Double exposure is also another major reason why cybercrime remains to be a challenge.[163] This leads to an exposure of an enormous number of accounts and passwords, as a result of data breaches, which continue unabated. Cybercriminals get personal information from the dark web, where they then attempt to access other accounts or help in blackmailing innocent individuals and organizations.

A unique challenge from cybercrime for policing cyberspace is the reviewing of the traditional approaches to the policing concept; apply new tools, both technical and legislative. Understanding traditional approaches affect investigation in the current times since the perpetrator of cybercrimes have already advanced their expertise and hence becomes very complicated to keep up with them by using the traditional approaches.[164]Other challenges faced include the development of skills of working with electronic pieces of evidence and the ability to cooperate with other industrial players. Another major issue entails capacity building. This is because the possession of new technologies for investigations and detection of crime does not necessarily mean the ability to effectively utilize them. This therefore calls for international cooperation amongst nations, both for government and non-government agencies, where they can effectively build a stronger role of international and regional police organizations such as the Interpol.

4.3 Difficulties in tracing offenders

There are multiple challenges faced in tracing the offenders. First, is due to the various possibilities of hiding identity in the international ICT network. There are also various tools that

[163] Ibid
[164] Ibid

the offenders use, whereby they have different ways of having anonymous access, surging, and communication.[165] This makes it very hard for law enforcement agencies to track them or even connect any individual to the crime.[166] The offenders also have the opportunity of using proxy servers, having unprotected public wireless networks, and managing to access anonymous communication services. There are also multiple criminals in different locations, making it very hard to investigate such offenses, which involve both the international aspect and hidden identity.

The internet is also designed to be governed horizontally and not vertically. The horizontal structure entails decentralized architecture which impedes control over activity on the internet. It hampers any type of investigation of cybercrimes. This hence requires both co-regulatory and self-regulatory approaches of the private sector and the owners and operators of the infrastructure.[167] Internet services and host providers are also very critical in making cybercrime investigations, where their cooperation is likely to bear fruit in addressing ICT-related problems. There is also a lack of borders in cyberspace and the international components of cybercrime. The question of criminal law in most cases is considered a matter of national sovereignty, where the protocols applied for internet data transfers are mostly based on optimal routing. This means that the process of transfer of data has to go through more than one nation, hence posing a huge challenge in tracking any person committing an offense through the use of these networks.

[165] Anderson, Ross, Chris Barton, Rainer Bölme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. "Measuring the changing cost of cybercrime." (2019).

[166] Ibid

[167] Tropina, Tatiana. 2009. "Cyber-policing: the role of the police in fighting cybercrime." *European Police Science and Research Bulletin · Special Conference Issue Nr. 2.* Germany.

4.4 Challenges facing law enforcement agencies in the fight against Cyber Crime

Law enforcement agencies have a major role in tackling the challenge of cybercrime in most nations across the globe, including Kenya and Zambia. As criminals are devising new ways of committing these crimes, it is a challenge to the law enforcing agencies who are faced by both traditional and modern challenges, hence making them unable to deal with the rising cases of threats.[168] First, there are many cases in which the police have been denied access to certain data or only have access to limited data, especially in the event of a criminal investigation. This makes them present weak evidence in the courts, and consequently the criminals may fail to get punished accordingly. The law enforcers are also faced with increasing technological development and internet use. This has resulted in a major challenge to them, whereby they are unable to detect the criminal or they face difficulties in distinguishing a specific user. Encryption is another tool that has proven to be mind-boggling to the enforcers. [169]By encrypting data, then criminals can stop incriminating data from getting to the hands of law enforcers. This hence makes it tough for the police and other enforcers to arrest or press charges for the criminals, due to lack of evidence. Others have adopted the use of cryptocurrencies such as Bitcoin, which helps criminals to deal with proceeds of crime, with a high level of anonymity. This shows that lack of data has led to a determinantal/ detrimental impact on the work of enforcers, which often results in investigations getting delayed or even discontinued.

Law enforcers are also faced with the challenge of loss of location. That is inability to easily detect the location of the perpetrators, any electronic evidence, or criminal infrastructure. This is easy when data gets encrypted, use of cryptocurrencies, and any other technologies. Loss

[168]Boes, Sanne, and E. Rutger Leukfeldt. "Fighting cybercrime: A joint effort." In *Cyber-physical security*, pp. 185-203. Springer, Cham, 2017.

[169] Ibid

of location means that the police will be unable to determine who was responsible for a certain cybercrime and hence be unable to easily make arrests or undertake an investigation of cyber threat.[170] In most cases, the criminals always outdo the law enforcers in terms of technical know-how hence making it hard to make a trace of them or access any incriminating evidence against them.

The law-enforcing agencies also face a major challenge of the legal frameworks in place. Sometimes it is hard to make investigations and prosecution of cybercrime cross- borders. Many cybercriminals operate globally, where without coordination of law enforcers across the borders, and then it may be futile to try to investigate and detect the cybercriminals. Countries may differ on the best approaches to cybercrime, making the coordination between law enforcers quite harder which as a result gives the cybercriminals an upper hand over the law enforcing agencies. The legal frameworks between nations may also be a conflicting factor that influences investigations. The lack of common legal frameworks between nations poses significant challenges for international cooperation. This is a major challenge since a case of large-scale cyber-attacks spans multiple nations and continents.

4.5 Public-private partnership challenges

There has also been an issue of public-private partnerships in fighting cybercrime, a factor that has affected the law enforcement agencies negatively. The private sector has the ability to providing with crucial data that can facilitate investigations. They can hence be very vital in helping the agencies to dismantle critical infrastructures. Despite the importance of the collaboration between the private and public sector, there lacks a legal framework that defines how

[170] Boes, Sanne, and E. Rutger Leukfeldt. "Fighting cybercrime: A joint effort." In *Cyber-physical security*, pp. 185-203. Springer, Cham, 2017.

the private sector can collaborate with law enforcement whilst at the same time ensuring that they do not breach the privacy or rights of their consumers.[171] This hence makes the collaboration a challenging factor that greatly favors the cybercriminals, since there are no frameworks from the collaborations that can stop them from undertaking their illegal acts. There are other further challenges associated with new and emerging technologies, such as the rise in the use of artificial intelligence and quantum computing. As much as this presents an opportunity to the law enforcers and also the private sector in detecting and mitigating crimes, it also poses a potential threat for criminals to misuses in fueling cyber-crime.

4.6 Challenges in prosecuting cybercriminals

Another major body that faces challenges in prosecuting cybercriminals is the judiciary. In many cases, cybercrime offenders are in different nations, which is outside the legal jurisdiction of the court and the prosecutors seeking the convention. It is therefore challenging for them to successfully prosecute a criminal of this nature, mostly as a result of the location of the offenders.[172] Jurisdiction of cybercrime offenses faces multiple challenges. For example, if a cybercriminal is in another country such as China and Russia, the nations may refuse to honor warrants of arrest, which would make it hard to have a successful prosecution.

Many legal systems are not well equipped to deal with the many cases of cybercrime. This is because internet crime was non-existence three decades ago. It is hard for the system to easily adapt to prosecuting such crimes, whose evolution is still ongoing, and which have not been

[171] Boes, Sanne, and E. Rutger Leukfeldt. "Fighting cybercrime: A joint effort." In *Cyber-physical security*, pp. 185-203. Springer, Cham, 2017.

[172] Naqvi, Syed. "Challenges of cryptocurrencies forensics: a case study of investigating, evidencing and prosecuting organised cybercriminals." In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1-5. 2018.

prosecuted before. [173] Some illegal online activities may also be permissible in some countries, making it hard to prosecute such crimes, especially if the crimes involve computers or people outside the jurisdiction of the courts. The legal systems have a hard task defining and prosecuting certain computer crimes, due to the lack of a particular standard in place.

Law enforcement is faced with the major challenge of getting cybercriminals extradited from one country to face prosecution. Despite working with other international agencies such as the FBI and Interpol, there still is a major challenge of extraditing anyone to answer the cases of cybercrime. This is not only a challenge faced by Kenya and Zambia but also other developed nations such as the US, where this is also a major. It is not a guarantee that a country will accept to collaborate to ensure that certain cybercriminal within their jurisdiction is prosecuted, or extradited to face trial.[174] An example is the case of the UK, where in 2018 it chose not to extradite a suspected cybercriminal, Lauri Loe, to the US, since he was experiencing mental-related issues.[175] However, the US has been successful in extraditing several criminals, across the globe including some from Africa. Countries across the globe do not have extradition treaties, meaning that the chances of bringing justice to someone in a new country are extremely low. This hence hinders the fight against cyber threats and gives the criminals a suitable environment to continue undertaking their criminal acts without the fear of getting arrested or prosecuted.

In most cases when gathering evidence for cybercrime cases, it takes very long delays. This is mostly in the event of dealing with internet facilitated bank frauds, where there are attacks

[173] Naqvi, Syed. "Challenges of cryptocurrencies forensics: a case study of investigating, evidencing and prosecuting organised cybercriminals." In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1-5. 2018.

[174] Ibid

[175] Davies, Gemma. "Court of Appeal High Court: Extradition, forum bar and concurrent jurisdiction: Is the case of Love a precedent for trying hackers in the UK? Lauri Love v (1) The Government of the United States of America (2) Liberty [2018] EWHC 172." *The Journal of Criminal Law* 82, no. 4 (2018): 296-300.

of software, and in most cases happens outside a country. The investigations and prosecutions require collaboration with other nations., As a result this leads to a longer time of gathering the evidence and undertaking the prosecutions. Law Enforcement Institutions may have inadequate digital forensic tools, which can help to easily gather electronic evidence. In some cases, the investigators may have to consult private cyber forensic firms, who aid them in conducting digital forensics. This results in delays in arresting, prosecuting, and sentencing the cybercrime perpetrators. The judiciary also lacks enough precedents of responding to the prosecution of cybercrime considering that it is a fairly new era. Many judges have not been trained on how to deal with cases of cybercrime, which is a major challenge to the fair sentencing of criminals. As much as many countries agreed to the Budapest convention on cybercrime, it is not a guarantee that all the cyber challenges will be addressed in a short period.[176] However, the convention provides a platform in which synergies can be built where member committees can cooperate and commit to communally provide stronger resistance to cybercrime. Working together for nations globally can help in weakening the front of the organized cyber-criminal activity for individual countries.

There has been a challenge of improper handling of electronic evidence. This can be attributed to the fact that some of the law enforcement agencies lack experience in gathering electronic evidence and complying with the legal admissibility rule in the specific country. As a result, this leads to most of the evidence presented in courts rejected. This is a factor that frustrates the efforts of fighting cybercrimes. This leads to recidivism. Failure to follow the right Chain of custody is another major challenge faced in the fight against cybercrime. The Chain of custody entails the process by which electronic evidence more so among various institutions. Many of the

[176] Patel, Durgambini A., and Sanjana Bharadwaj. "Budapest Convention on Cyber Crime." (2020).

times, the evidence fails to go through the proper custody chain hence fails to be admissible in the court.

The prosecution of cybercriminals has also multiple times been affected by the unwillingness of the witness to testify in most cases where they fear being stigmatized or lose clients. The witnesses are drawn from banks, insurance companies, and the automobile industry, who are often not willing to pursue cases when they face cyber-attacks fearing that their companies may face negative publicity and ultimately lose their clientele. This limits the success in prosecuting cybercriminals. This is a threat to the success in the war against cyber threats.[177] In the event of cyberbullying, women (mostly) who may have faced such types of threats, may be unwilling to testify due to the stigmatization attached with such cases. In most cases, in Kenya, Zambia, and the rest of Africa, parents, religious leaders, and even community leaders may try to settle this out of court.

4.7 Lack of Resources

A major challenge hindering the successful fight against cybercrime is the lack of resources to help in the investigations, arresting, and prosecuting of any cybercrimes. There also lacks manpower and skills to investigate the crimes globally. The law enforcing agencies as a result focus their time and efforts on other bigger cases which they know will have successful prosecutions and fail to focus on cybercrime. As a result, the cases continue to escalate, wherein the recent times there has been a growth in cases of cyberbullying, child sex crimes, and other incidences that result in multiple financial burdens to the government, innocent civilians, and

[177] Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International Journal of Critical Infrastructure Protection* 25 (2019): 36-49.

institutions. [178]The law enforcement agencies fail to focus on the smaller crimes where they as a result create a sustainable environment for their growth to bigger cybercrimes.

4.8 The challenge of the modern technology

Technological developments have seen an evolution in the way people conduct their things. The 21st-century has marked acceleration in both the online world and the threats that arise from it. The technological programs have numerous capabilities of programs and a wide range of services. As a result, they have brought technical, political, economic, and social challenges, where malware has resulted in a higher frequency of issues than it cures. This means that the number one challenge that faces the fight against cybercrime, despite the efforts made by both state and non-state actors, has become exceedingly difficult to control over targets and attackers. There continue to be more complex hacking tendencies, which often target critical objects both private and public. Growth in the cyberspace functionalities has given terror groups the capabilities to develop, access, and increased motivation to target states and private infrastructure. According to many reports, research, and intelligence information gathered, the future may also be full of threats of the terrorists as they continue to acquire enhanced skills to use cyberspace for attack purposes.

Another challenge faced by state and non-state actors is the limited research on the topic of cybercrime. The subject of cyber terrorism is situated within limited fields of research, meaning that specific publications on the topic are limited. [179]As much as in recent years, there have been multiple studies conducted to explore sustainable solutions, there still is a huge gap in the research, that could offer help the agencies address the issue with sustainable solutions. Authors of certain

[178] Jhaveri, Mohammad Hanif, Orcun Cetin, Carlos Gañán, Tyler Moore, and Michel Van Eeten. "Abuse reporting and the fight against cybercrime." *ACM Computing Surveys (CSUR)* 49, no. 4 (2017): 1-27.

[179] Nouh, Mariam, Jason RC Nurse, Helena Webb, and Michael Goldsmith. "Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement." *arXiv preprint arXiv:1902.06961* (2019).

publications, doctrines, governments, and other international organizations often differ in opinion on ways of tackling cyber-crime and the consequences of cyber-crime may have on institutions and innocent civilians.   There is controversy in the existing literature e, which is largely based on the impossibility of defining appropriate terms to use when addressing cybercrime and also fitting the terms in the existing legislation or into the policy of a country on cyber welfare.

Some of the law enforcement and security agencies fail to share specific information with other stakeholders, which would help in a cohesive working environment. In most cases, the agencies cite high threats associated with the sharing of such information. However, this limits the collaborative efforts, which can only be attained when the various agencies both in the public and private sector work together to realize the set goals. Despite the failure to share information, the security agencies have confirmed that terrorists continue to acquire sufficient expertise in performing attacks on cyberspace. By getting such sophisticated know-how, then they may easily threaten nations, and could easily attack without getting detected by the security agencies. It is highly likely that nations are likely to cyberattacks that emanate from cybercrime perpetrators and terrorists.

The issue of the legality of the response to cyber terrorism is also another major issue challenging the success of the fight. This is because some regulations may face court restrictions especially if they appear to be unconstitutional or affect innocent civilians negatively. [180]In Kenya, for example, there have been numerous court cases opposing a newly drafted cyber bill, which had clauses that were opposed by civil society. In many nations, the law in place tends to put unnecessary restrictions and acts as an impulse for disagreements on activities in cyberspace.

[180]Evans, Caleb. "The Legality and Considerations of Countering International Terrorism." *Oklahoma City University's Undergraduate Research Journal*: 73.

In many cases, when the time comes to act in the protection of civilians and a nation, especially when fighting against cyber threats, it gets hard to depend on the legality of the response. The current legal frameworks are not effective enough to help in ensuring that there is justice when fighting for justice and ensuring that the cybercriminals are punished accordingly and that justice is fully served.[181] The problem in place is not the absence of law, but rather the application of facts and complexities to the frameworks which make rendering justice difficult.[182]

There have been proposed acts on ensuring that cyberspace is safeguarded, but legislators oppose, or other non-state agencies in courts. This is since some of the facts may have clauses that appear to be intruding on the business of private companies and affect the private lives of the citizens individually. It appears that when the threat of cybercrime gets bigger, then there is an increase in reluctance by the policymakers to reach a compromise when enacting such a law.

The growing concern about cybercrime and cyber terrorism has resulted in increased implementation of legislation and countermeasures to deal with perpetrators and prevent future attacks by both non-state and state actors. However, these measures have been accompanied by a wide range of challenges. One such challenge is as a result of the anonymity that is accorded to users by modern information and technology. Cybercriminals can use anonymous networks to hide their IP address and encrypt traffic. It is therefore easy for them to conceal their illegal activities and transfer them from one state to another. The anonymity privilege makes it hard for law enforcement agencies to detect these activities. It is therefore becoming impossible to detect or

[181] Ibid
[182]Tereshchenko, Natalia. 2013. "US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure." https://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/.

track any criminals conducting malicious activities on the internet. [183]Cyber terrorists can continue with their operations in a borderless environment without being detected by legislators. Additionally, political ideologies and foreign policies limit the existing competencies developed by the state to deal with cyber-terrorism. Law enforcement agencies especially in third world nations are further limited by inadequate resources and funding as well as a lack of trained personnel to deal with cyber-terrorism. These challenges make it impossible for law enforcement agencies to provide adequate deterrence for any cyber-terrorism activities.

4.9 Harmonization of cyber laws

Harmonization of cyber laws is vital in the war against cybercrimes since it allows the different concerned bodies to collectively organize their resources and effectively combat cybercrime. According to UNCTAD, the different legal systems need to be compatible and interoperable for actors to enforce related laws both domestically and internationally. However, many states suffer from the lack of harmonized national laws, which in turn, affect limit, their ability to fight cybercrime and cyber-terrorism. The lack of compatible agencies also harms the allocation of resources needed to fight cyber terrorism. Additionally, for a long period, states have been unable to develop and adopt compatible e-transaction laws. E-transaction laws are vital in conducting online financial transactions. Hundred forty five(145) states especially those from transitioning and developed economies, including Latin America and Asia have fully adopted these

[183] Nuredini, A. (2014, August). CHALLENGES IN COMBATING THE CYBERCRIME. *Mediterranean Journal of Social Sciences, 5*(19), 592-600.

laws.[184] However, countries especially those from Central and East Africa lag due to inadequate resources and unstable leadership.

Other outcomes of incompatible laws and agencies result in a lack of timely collection of needed information and slowed process in regards to sharing digital evidence between states which act as obstacles to the investigation process. In certain instances, cybercrimes are politically motivated. In such states, leaders and politicians lack the general will of cooperation. Additionally, cyber-crimes are sophisticated and legally intricate; the differences of each state's legal and technical systems result in complex challenges.[185] In most states there are is no single jurisdiction approach to policing when it comes to responding to cybercrime. The result is increased ease of movement for cybercriminals; a movement that has gradually become a significant challenge for state and non-state actors batting? the misuse of cyberspace.

A ruling made in April 2014 advocated for the overturning of the Data Retention Directive (DRD), making it impossible for investigators to obtain information and data from private sources. In some EU member states, legislation to retain data using IPS for investigation purposes was annulled in the wake of the European Court of Justice (CJEU). In such states, there is no available data to support cyber terrorism investigations. These discrepancies impeded the investigation processes and may result in false leads and affect a state's ability to curb cyber-terrorism activities.[186] Additionally, the CJEU'S ruling in December 2016 pressured investigators to

[184] Europol, & Eurojust. (2019). *Common challenges in combating cybercrime.* Europol and Eurojust Public Information.

[185] Nuredini, A. (2014, August). CHALLENGES IN COMBATING THE CYBERCRIME. *Mediterranean Journal of Social Sciences, 5*(19), 592-600.

[186] Europol, & Eurojust. (2019). *Common challenges in combating cybercrime.* Europol and Eurojust Public Information.

priorities their investigations per the existing data retention frameworks instead of paying more attention to the high-value targets.

There are different technical challenges faced during the investigation processes. Investigators require a wide range of digital devices including hardware and software to obtain, conserve and transfer digital evidence. However, in most instances, they may lack these devices and digital forensic tools that are used in collecting digital evidence. [187]Back-tracing is another common technical challenge. Through back-tracing, investigators can monitor and track down malicious activities back to the perpetrators or the digital device being used. They can also track down the location of the perpetrator. This process is carried out after a crime has occurred. Unfortunately, the process is time-consuming and is highly dependent on the skills and knowledge applied by the perpetrators.[188] In most scenarios, the perpetrators take great measures to conceal their activities and identities making it impossible for investigators to trace the acts to not even one identifiable source. Most of these investigators are not equipped with modern skills and knowledge to fight back these perpetrators.

While modern technology has had a massive impact on different sectors of life including making it easy to detect and identify cybercriminal activities, it has become a great enabler for cyber terrorism. With the invention of cryptocurrencies such as Bitcoin, criminals can make anonymous transactions and conduct illegal activities such as Distributed Denial of Service (DDoS) attacks without being detected. There is an increased use of decentralized cryptocurrencies that have minimized the possibilities of detection and prevention of fraudulent transactions. Most

[187] Eggers, W. (2016). *Government's Cyber Challenge.* Deloitte Review.

[188] Brunner, M. (2014). Challenges and Opportunities in State and Local Cybercrime Enforcement. *JOURNAL OF NATIONAL SECURITY LAW & POLICY, 10*, 563-583.

states lack the needed due diligence and the standard for Know-Your-Customer (KYC) needed for investigations. The increased use of current trends such as cryptocurrencies and anonymity tools has challenged the ability of authorities to trace the physical locations of the perpetrators. The situation is further made worse in countries with unclear jurisdiction and legal frameworks that enable the collection of timely digital evidence. Additionally, the introduction of cloud-based storage and services implies that information stored in the cloud could be traced back to a different jurisdiction, further worsening the ability of authorities to locate the exact location of perpetrators.

In recent years, states are cooperating with the private sector in combating cyber terrorism and crime. This partnership is essential in mitigating cyber-attacks while also increasing awareness among the larger population. However, there is inadequate consensus in regards to the current legal framework needed to facilitate a trust-based partnership between the two parties. There is a need for the introduction of standardized rules of engagement between the public and the private sector. There is also a need for rules that stipulate the extent to which private parties can go to gather digital evidence and the implications for the actions taken. Unfortunately, most states are yet to strike a legislative balance between the needs of the public sector and the private sector as well as the proportionate measures that guide the support given by the private sector to the law enforcement agencies. Additionally, the private sector is not well informed about the transparent rules that guide their involvement and actions such as the admissibility of digital evidence corrected in court proceedings.

4.10 Why SMEs Leaders contribute to increased vulnerabilities

In Kenya and Zambia SMEs have been one of the biggest targets by hackers and other cybercriminals. However, many of them continue to assume that they are small in size as compared to large businesses and that they are unlikely to be targeted by criminals. Their leaders perceive that their businesses are somehow immune to cyber-attacks and data losses. According to Cisco 2017, small organizations that are yet to suffer from security breaches may believe that their networks are safe.[189] They hence fail to undertake safety measures that will help their business protected from attacks also fail to undertake measures advised to them by the governments and other non-state actors in place. They also fail to participate in forums that address matters concerning cybersecurity and do not collaborate with security and other non-state organs in the fight against cybercrime. Most SMEs do not have a proactive sensitization and appreciation of cybersecurity, which would help in having safe cyberspace. This is hence a major challenge faced in the fight against the threats.

Cybersecurity threats towards SMEs in Kenya and Zambia continue to increase at an alarming rate. In most cases the crimes are not detectable; therefore, criminals get away without getting prosecuted. Several enterprises do not have experts who can help them in detecting or preventing the attacks. Employees are not trained on the best ways of dealing with the shifting ICT systems, which is also another major challenge faced by SMEs. The ICT systems that can help in fighting the crimes are also expensive, making it hard for them to defend themselves against the crimes. Failure to invest enough for SMEs in Kenya and Zambia particularly is another bigger threat and challenges faced in the fight against cyber threats and cyber-terrorism. Some leaders have limited strategic directions which they need to implement to ensure that their business systems are securer. Many have failed to undertake cyber strategic leadership actions that can help be involved in the cybercrime war.

[189] Ndeda, Laureen Akumu, and Collins Otieno Odoyo. "CYBER THREATS AND CYBER SECURITY IN THE KENYAN BUSINESS CONTEXT." (2019).

The SMEs have very meager budgets t for fighting cybercrimes, where 90% of organizations in Kenya are allocating less than Kshs 500,000 annually for cyber-security measures.[190] This is proof that there are not enough investments in the fight against cybercrime, hence contributing to the growing cases of attacks for the small and medium enterprises in the region. Leadership is another challenge faced in the fight against cybercrime. Many leaders are not conversant with the importance of having cyberspace strategies (is there empirical evidence?). Many SMEs neglect important areas such as business continuity, disaster recovery, and legal compliance. [191]These factors are critical issues in the current cyber era and can help SMEs to deal with the threat by having sustainable solutions and adhering to the directives on the threats. This is proof that many of the SMEs take advantage of technology in automating various functions but are not aware of the various cyber threats associated with the automation, where it encourages cyber strategies which prepare for the threat eventualities.

Sufficient training and development strategies on cyber threats, leaders who have the utmost knowledge need to understand the most suitable cyber strategies to undertake and as a result adopt measures of countering the threats. Few government awareness efforts can help institutions participate in familiarizing themselves with the threats.[192] The awareness programs could include training of cybersecurity skills and creating knowledge on what to do best as a way of counter-attacking the threats and making a business threat-free.

[190]*Serianu. (2015). Kenya Cyber Security Report 2015. Nairobi, Kenya: Serianu Cyber Threat Intelligence Team. Retrieved March 18, 2018 from http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf.*

[191] Ibid

[192]Njoroge, George M. "Human Factors Affecting Favourable Cybersecurity Culture-a Case of Small and Medium-sized Enterprises Smes Providing Enterprise Wide Information Systems Solutions in Nairobi City County in Kenya." PhD diss., University of Nairobi, 2020.

4.11 Reason for not adopting cyber-security to provide enhanced secure cyber-space

As much as lack of finances to fight against cyber threats can be attributed to the lack of adopting cybersecurity measures, there is also poor management by the leaders of many businesses. Many leaders in small and medium enterprises fail to show great leadership on matters of cyber policies, where they could advise their juniors on the best measures to undertake in the fight against the cyber threats faced by these businesses.[193] Many businesses lack cybersecurity skilled workers, who would help in ongoing proper directions on businesses on the way forward in the fight against increasing cyber threats. Poor infrastructure in business can also be attributed to the increasing threats, where the cybersecurity systems at most business are poor and outdated, hence easier for the criminals to target. [194] Many of the SMEs lack structured frameworks, which would help a business understand the best ways and strategies of countering the cyber threats and ensuring that everyone within the organization is conversant with the most suitable ways of fighting the crime.

There is a major challenge of lack of cooperation from service providers, who in most cases are from the private sector. As much as they have logs and records, which could have helped the agencies, identify the criminals, they fail to provide them, citing the law on the right to privacy. In the logs, are destination addresses, billing records, duration of services, and the types of services, which can easily help identify a local cyber-criminal. Other providers fail to follow the law on some of the provisions on privacy and the powers they have in demanding compliance from the service providers.[195] The misunderstanding of the laws in place concerning cybercrime is also

[193] Muhati, Eric. "Factors affecting cyber-security in Kenya–A Case of Small Medium Enterprises." PhD diss., Strathmore University, 2018.

[194] Ibid

[195] Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International Journal of Critical Infrastructure Protection* 25 (2019): 36-49.

another major hindrance that makes it hard to establish sustainable solutions to cybercrime in the region.

Investigations of cybercrime are complex, where there is the requirement to gather evidence as a way of prosecuting cyber cases. Some of the undetectable ways used to malign health businesses by cybercriminals include sending harmful links, using the internet to harm competitive businesses and many other ways which are hard to trace the primary source of information. The agencies mandated with fighting cybercrime, are often unable to get the source of information even within a country. It gets even more complex when the service provider is outside the jurisdiction of a country where there the agencies will have to rely on mutual legal assistance requests.

4.12 Conclusion

Multiple challenges are facing both the state and non-state actors in the fight against cybercrime. The misuse of technology has created multiple problems and risks for individuals and groups in society in general. It has also brought national safety to a major risk. It has resulted in a change in how offenders who commit crimes are approached. The digital general approach had opened new opportunities for unscrupulous behaviors. A lot of money has been lost by businesses and customers through the use of computers, which is a part of the commission of a crime. Perpetrators are easily using computers and other networks to attack unknowing victims, prepare for global violence such as terror attacks. Lack of enough trained personnel to deal with the threat is hence a major challenge. This is since they are easily changed by specialized cyber offenders, who are easily able to access classified information and use it against companies or even individuals. There is hence a need for thorough research on the best sustainable solutions that will help in identifying sustainable solutions that can help in the fight against cybercrime.

CHAPTER FIVE

RECOMMENDATIONS AND CONCLUSIONS

From all the chapters, it is manifest that Cybercrime is a major challenge faced by African nations including Zambia and Kenya. Multiple businesses and consumers in these economies are facing increasing cyber threats. There is hence a need to strengthened cybersecurity measures. There is a need for organizations to increase their investments in cybersecurity technologies. First, companies need to provide cybersecurity-related training to workers and appoint professionals such as CISOs.[196] There is also a need to create cybersecurity awareness programs that will help the consumers enhance their knowledge on the matter. There is a need for policymakers to focus on public awareness of cybersecurity practices and strengthening regulatory and enforcement capabilities in this area. There is a need for regulations to ensure strong cybersecurity measures in organizations.[197] The regulations ought to be continually raised, as a way of coping with the shifting changes in the tactics of cybercriminals.[198] There is a need for more initiatives that will focus on enhancing law enforcement capacities, to increase the certainty of punishment for any individual engaging in acts of cybercrime activities.

Both state and non-state actors need to collaborate in coming up with measures on counter-attacking cybercrimes. First, they should collaborate with the policymakers to ensure that they work together in increasing public awareness of cybersecurity practices and strengthening

[196] Union, African. "A global approach on Cybersecurity and Cybercrime in Africa." (2015).

[197] Ibid

[198] Tereshchenko, N. (2013). US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure. Retrieved from https://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/

regulatory and enforcement capabilities. There is a need to have potential fruitful revenues for future research. Cybercriminals are targeting developing economies including Kenya and Zambia. There is a need for future conceptual and empirical work scholars need to compare and contrast economic sectors facing high profile cyberattacks in major African economies with those in non-African developing economies.

5.1 More Funding and allocation of Resources

Another primary recommendation that would greatly help in combating cyber threats in Kenya and Zambia is the increase in funding allocation. More resources significantly help in enabling the implementation of the strategies in place. This is because implementing the plan will allow Kenya and Zambia to realize their set goals and visions, which can only be made possible if the government and the private sector work to ensure that the programs are well funded and resourced. Therefore, the ministries of finance will need to allocate enough funding, depending on the type of implementation strategies in place.[199] The government needs to play more roles in the fight against cybercrime by allocating more resources to the courses which will help in the fight. The resources are important in that they help to invest in research, which helps in developing suitable innovations that will ultimately help in developing sustainable solutions towards fighting cyber threats. The government also can influence the SME to participate in enhancing secure cyberspace, through holding campaigns and practicing safety measures that will ensure better cybersecurity. [200] The government also can strengthen its institutions, including the law enforcing

[199] Business Daily Africa. NOVEMBER 19, 2012. "Kenya steps up fight against cyber-crime." https://www.businessdailyafrica.com/bd/corporate/companies/kenya-steps-up-fight-against-cyber-crime-2019556.

[200] Community Authority of Kenya. 2019. Cybersecurity meeting calls for expedition of Data Protection Bill and investments in more professionals. https://ca.go.ke/cybersecurity-meeting-calls-for-expedition-of-data-protection-bill-and-investments-in-more-professionals/.

agencies and the judiciary, who in return can ensure that cyber criminals are arrested and effectively persecuted, hence reducing the rate of crime. The government through the legislature on the other hand can ensure that there are enacted cyber laws, which help in effectively dealing with cybercriminals. The legislature together with other stakeholders in the private sector needs to ensure that they collaborate in the development of these policies since they will help in making the cybersecurity war a success.

5.2 Creation of Awareness

There is a need for the governments to also increase their awareness campaigns on national roadmaps, which will be geared towards protecting business resources since most SMEs are eager to engage and exchange cybersecurity assets. The government should focus on SMEs and see them as the most vulnerable in the country and require extra security measures to ensure that they are capable of withstanding any type of threats.[201] As much as there have been multiple studies on cybersecurity, there is a need for more to establish more innovative and sustainable measures that can help protect businesses, government institutions, and individuals from attacks.[202] It is manifest that Cybersecurity can only be improved as a collective effort between SME leaders and the government. In the future, there is a need for a study that will focus on evaluating cyber-security adoption in Keya and Zambia as a way of understanding the same independent variables that differ in impact on cyber-security adoption and cyberspace.

[201] Connolly, L. Y., and D. S. Wall. 2019. "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures." Computers & Security 87, 101568.

[202]OBURA, F. (November 8th 2020). Kenya steps up fight against cybercrime. Retrieved from https://www.standardmedia.co.ke/business/sci-tech/article/2001393164/kenya-steps-up-fight-against-cybercrime

In the future, there will be a need for campaigns for awareness programs to all citizens within a country on how to enable them to protect themselves and their data from cybercrime. Some of the issues that such campaigns should address include the use of strong passwords, securing their computers, blocking spyware attacks, and being a social media survey. Social media is also another critical tool that can help in the fight against cybercrime, where many people are on one or more platforms.[203] This is a significant way of boosting knowledge and creating awareness to the public on preventing themselves from being easy targets to the criminals. Other tactics to be emphasized in the awareness campaigns will include the need for people to secure their mobile devices, being careful with what they post online, download applications from trusted sources, installing the latest operating system updates, and keeping their applications and operating system current with the latest system updates.

The use of encryption for data, protecting identity, and securing a wireless network, will also be great tools to help people avoid any cases of attacks or cyber threats. The media coverage is vital too that it can also help curb the increasing rates of cybercrime. More needs to be done by the media to ensure that the public gets more knowledge pertaining to cyber threats and how they can protect themselves.[204] Both the state and non-state actors can approach media houses, issue important warnings, share information, and create awareness of the need to be aware of possible cyber threats, since this will easily reach the public and help minimize the cases of cyber threats.

[203] Ismail, Nick. 29 January, 2018. "Collaboration is key in fighting cybercrime." https://www.information-age.com/collaboration-key-fighting-cybercrime-123470569/.

[204] Eweniyi, Odunayo. 2014. "Kenyan Government Joins the Fight Against Cybercrime." https://techcabal.com/2014/05/07/kenyan-government-joins-fight-cybercrime/.

Nevertheless, it is manifest that cybercrime cannot be fought by any law or holding conventions alone. A collaboration of all levels of stakeholders in the government and nongovernment organizations is necessary.[205] There is also a need for the operation of the internet, to help in the protection of the privacy and security of internet users. There is a need for a secure and safe environment to be shared, where it is collective responsibility within the continent. It is also important in that it can help in ensuring that there are multiple benefits of the digital transformation of Africa to support both human and economic development.

There is a need to encourage a strong security culture amongst the government and within businesses. Through a collaboration of the state and non-state actors, then a well-laid security culture will be effectively implemented and hence help in securing the various systems in place. Governments must also understand that many of those carrying out hacking attacks are mostly young, talented, and alienated from wider society, where it should focus on enhancing their skills should be recognized and nurtured as part of a national response to cybercrime.[206] It is evident that in the future, there is a high likelihood of more cyber-attacks, due to the growing technology and increasing creativity and innovation amongst the perpetrators of the attacks. This will hence require more effective strategies by the governments and other non-state actors who will require to have a new international strategic and operational partnerships as a way of securing the systems.[207] The active partnerships with the private sector will be very essential in that it will help

[205] Ismail, N. (29 January, 2018). Collaboration is key in fighting cybercrime. Retrieved from https://www.information-age.com/collaboration-key-fighting-cybercrime-123470569/

[206] Jakobi, A. P. (2013). Non-State Actors All Around: The Governance of Cybercrime. 129-148. doi:https://doi.org/10.1057/9781137334428_7

[207] Eilstrup-Sangiovanni, M. (2018). Why the World Needs an International Cyberwar Convention. *Philos. Technol*, 31, 379–407. doi:https://doi.org/10.1007/s13347-017-0271-5

in the sharing of intelligence and evidence and also aid in the development of technical tools and measures for law enforcement which will ultimately help in the prevention of online criminality.

5.3 Improving Government structures

There is a need for restructuring the government structures to improve efficiency in the fight against cybercrime. There is a need for a multi-stakeholder National cybersecurity council, which will entail representatives from private and relevant government agencies. Such a commission will be vital in that it ensures that the country has the best preventative measures of fighting cyber threats and ensuring that the government is well-prepared in an attack. There is also a need to establish a Computer Incidence Response Team, which will work together with the Council. It will undertake the duties of observing likely threats and attacks and consult on the best ways to ensure that sustainable solutions are in place.

A cybersecurity operation center needs to be opened both in Zambia and Kenya to ensure a central management center that helps fight against any threat. Such a center is vital because it deals with the highest-level threats, where they will eb enough skilled personnel that will help manage the levels of threats. A cybersecurity operation center can help monitor the attacks, evaluate the objective of a threat, protect and preserve the sovereignty and economy of the two republics. [208] The center will also be mandated to understand the state of the attacks, such as state sponsored or non-state actors' activities that include terrorism. The center will need to be managed by the National security agencies given the nature of its assignment. One of such a center's features will include a digital forensic library, which will aid in the processing and analyzing electronic

[208] Korir, Cheruiyot. November 29, 2016. "Government to curb cyber crimes." https://ict.go.ke/government-to-curb-cyber-crimes/.

devices that will help curb any future attacks. This will be by incorporating law enforcement agencies in the cybercrime department, leading to such a library.

Kenya and Zambia's governments need to undertake more roles in ensuring sustainable solutions in the fight against cyber threats. They need to assume the role of including national-level structures and participate in the citizen-level capacity building[209]. They need to undertake numerous campaigns, which will ensure that citizens know that cybersecurity is everyone's responsibility. The governments need to collaborate more with the private and independent stakeholders to ensure that they have a leading and critical role in ensuring Security in the cyber space as a team. The receptive ministries, including the ministry of ICT and internal Security, need to work together with the legislatures to constantly develop relevant policies and strategies, which will help in the development of laws that will aid in the fight against cybercrime, which will help in improving the ICT sector in the respective countries. [210] The governments will also be mandated with coordinating and implementing the laws through the National, regional and global collaborative efforts, which will help enhance local resources and encourage talent and innovation without the fear of attacks. The governments will also play a massive role in oversight the ICT sector and ensuring that there is an overall coordination between respective agencies to help curb cyber threats.

There is a need for various ministries to come together and work towards having the most suitable mechanisms to ensure that there are appropriate measures in place to curb the growing

[209] Nadir, I., and T. Bakhshi. 2018. "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. In 2018 International Conference on Computing, Mathematics and Engineering Technologies." 1-7.

[210] OBURA, FREDRICK. November 8th 2020. "Kenya steps up fight against cybercrime." https://www.standardmedia.co.ke/business/sci-tech/article/2001393164/kenya-steps-up-fight-against-cybercrime.

threat of cybercrimes. Some of the most relevant ministries include the Ministry of ICT, the Ministry of Internal Security, and the Ministry of Defense, ensuring that sustainable measures are in place. Their collaboration is relatively easy to assess the cyberspace landscape and identify the likely threats and risks.[211] This will help make sure that law enforcement agencies and other security services are in place to combat cyber terrorism and maintain law and order in cyber-attacks and emergencies. The ministries will need to collaborate with the legislature and the judiciary to ensure that there is a justice system in place and that sustainable law enforcement of cybersecurity-related laws is in place to aid with the investigations and prosecution of cybercriminals.[212] The judiciary will need to continually be kept abreast with the latest changes and developments related to cyber laws to ensure that it takes part in dispatching appropriate justice. There is a need for constant updates of rules, procedures, and policies to address emerging incidents and respond to the threats accordingly.

Both Kenya and Zambia need to have a strong Council for the coordination and implementation of cyber strategies. The Council will collaborate with the ministries, agencies, departments, and the private sector to ensure that the implementation succeeds. The Council will also need to ensure that it promotes more public-private sector collaborations towards ensuring a robust national security approach. It will also be mandated to provide strategic leadership to all the relevant agencies in both state and non-state departments. The Council will consist of all critical stakeholders conversant with cybersecurity matters from both the private and public sectors.

[211] Tan, Aaron. 2017. "Collaboration is key to combating cyber crime." https://www.computerweekly.com/news/450421906/Collaboration-is-key-to-combating-cyber-crime
[212] Xinhua. 2020. "Kenya to partner with private sector to boost cyber seurity." http://www.xinhuanet.com/english/2020-11/06/c_139496641.htm.

5.4 Incorporating civil society in Decision Making

Civil society plays a crucial role in making sure that there is the right to balance protecting civil liberties, human rights, and privacy rights in the implementation of cybersecurity strategies. There is a need for the government and other non-state agencies to incorporate civil society in their decision-making on cyber security matters. The importance of civil society is that it provides confidence and integrity and ensures that the measures undertaken on national cyber-security do not tramp on civil liberties.[213] Multiple civil service societies have been established globally to address the issue of cybersecurity and crime. An example includes the societies that deal with online Child protection. Therefore, establishing solid collaborations with these societies enables the successful implementation of strategies. It also aids in creating a balance between doing what is ethically correct and having suitable measures for protecting the citizens against cyber-attacks.

5.5 Collaborating with the private sector

More collaboration with the private sector is essential for the effective implementation of strategic measures against cybercrime. By collaborating with the private sector, businesses will be expected to implement adequate cybersecurity safeguards into their practices and operations. Undertaking such precautions will primarily entail enhancing technical solutions and adopting the best procedures to secure business processes. Some of the most critical sectors include the financial and banking industries, which ought to accord high priority to cybersecurity since they are likely to be attacked or face external threats.[214] The private sector has a vital role to play, and hence by

[213] KENYA GAZETTE SUPPLEMENT. 2018. The Computer Misuse and Cybercrimes Act, 2018. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf.

[214] Quarshie, Henry Osborn, and Alexander Martin-Odoom. 2012. "Fighting Cybercrime in Africa." 2(6): 98-100. doi: 10.5923/j.computer.20120206.03.

collaborating with state agencies, it will help develop cyber security business norms, codes of conduct, and standards. It will also help in identifying and also encouraging the adoption of good practices. Together with the relevant agencies and stakeholders, the private sector can help develop innovative methods and technical standards of protecting Security. This can be made possible by taking part in appropriate forums or standards-development. The private sector can also collaborate more with state agencies to receive equipment, identifying technical solutions that help protect digital infrastructure and information.[215] The collaboration can also help the private sector have more information regarding new cyber threats and create awareness on suitable countering methods. Information can also help the industry in ensuring compliance with the minimum cybersecurity standards.

There is a need for more increased private-public partnerships in the future to bring more positive change to the fight against cybercrime. This is since more collaborations help develop innovative ways and new strategies that will understand the motive and ways of cyber criminals, hence helping in combating major cyber threats. This may include increasing the number of CERTs, which will help aid the private sector industries with any issue related to cybercrime. Such public-private interfaces will significantly facilitate intelligence sharing and collaboration.

To ensure that sustainable solutions are attained in the fight against cybercrime, there is a need for public to change attitude. Both state and non-state actors have a role in empowering and creating more awareness to the public on the need to be aware of online fraudsters and threats that

[215] Tereshchenko, Natalia. 2013. "US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure." https://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/.

are likely to affect them adversely.[216] There need to institute more programs that create awareness to the general public on Online fraud, social engineering, theft, and impersonation, which have become a significant threat, more so due to the rising cases of online activities across the globe. The public needs to be aware of phishing sites, spam emails, and scams to prevent them from getting conned or attacked by cybercriminals.

5.6 Role of the financial institutions in combating cyber crime

Due to the high threats, they face, financial institutions need to make positive changes both in Kenya and Zambia. They need to undertake more measures of safeguarding their transactions and fund transfer areas. They also need to ensure that the cybercriminals do not use their facilities to facilitate money transfers and cash outs. Financial institutions also need to share more threat intelligence information between themselves, the state agencies, and other key stakeholders. Discussing the likely threats is vital to understanding the latest developments in cybercrime and combating them.[217] They need to be conscious of what they can legally share within the regulatory framework to ensure that they are within the right frameworks and that the criminals do not get access to their information and strategies.

Sharing information about cyber threats among financial institutions helps them focus on sharing the most suitable ways of protecting the customers and helping the banks detect and stop fraudulent activities. It also dramatically helps law enforcement obtain evidence needed for successful arrests and the prosecution of cybercriminals. As much as many institutions have

[216] National Cybesrsecurity Strategy. 2014. Ministry of Information Communications and Technology. http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf.

[217] Nikkel, Von Bruce. 2018. "Positive Changes and Collaboration in the Fight Against Cybercrime." https://www.societybyte.swiss/en/2018/01/22/positive-changes-and-collaboration-in-the-fight-against-cybercrime/.

already commenced sharing information, they need to do more for further collaborations to establish sustainable solutions.[218] There is a need for increased awareness and understanding of criminal activity among financial institutions and banks. This can be made possible by enhancing the relationship between the clients and the managers, who should be vigilant and suspicious of likely illegal activity. Communicating to the financial institutions in such events can help in combating cyber threats at the financial institutions. All banks and financial institutions need to be encouraged to invest more in their overall Security.[219] This includes the development of analytical systems, defense mechanisms, and anomaly detection systems. This is to protect themselves and their clients. They also ought to invest in having dedicated teams and engaging insurance companies to add cybercriminal incidents to their insurance portfolios.

5.7 Government and Law Enforcement Changes

There is a need for more cross-border and cross-jurisdiction collaborations as a way of combating cyber threats. Law enforcement agencies need to reach out to other agencies within a country to improve efficiency. There should also be more international collaboration with international agencies to undertake investigations across the borders. This could be by engaging agencies such as Interpol and Europol, who could help in undertaking transnational cyber-crimes, which are on the rise. [220] The collaborations with the international agencies and the private sector agencies can ensure a multiagency approach, which will ensure that all offenders, despite the

[218] Ibid

[219] Nikkel, Von Bruce. 2018. "Positive Changes and Collaboration in the Fight Against Cybercrime." https://www.societybyte.swiss/en/2018/01/22/positive-changes-and-collaboration-in-the-fight-against-cybercrime/.

[220] Ibid

country they are operating from, are arrested and punished accordingly. The Government and law enforcement can share relevant information, which will help in smooth investigations.

More training and development programs need to be undertaken for the law enforcement agencies in Kenya and Zambia to help them understand the magnitude of cyber threats and understand their role in combating the threats. They ought to be made conversant with the latest technology-based crime. They need to understand about botnets, phishing, and malware among many other technologically complex criminal activities, and also be made to know how their prowess can help in combating them. Through training and development programs, they will be able to improve their investigation abilities. Through training and development, they will be able to get a better understanding of the IT operations of the private sector. They will understand how to manage great collaborations without compromising any institution or citizen. Through training, the law enforcement agencies can also have a smooth interaction with other agencies, which will eventually help in the successful investigations.[221] The programs can entail combining both government and non-state agencies to. There is a need for law enforcement agencies to be aware that criminals themselves are changing tactics over time. They have become more organized and industrialized where they have an organized underground economy. They also have innovative ways of distributing malware, recruiting money mules, and other tactics.[222] As a result, law enforcement must constantly upgrade its practices to keep up with criminals changing tactics.

[221] Tereshchenko, Natalia. 2013. "US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure." https://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/.

[222] OBURA, FREDRICK. November 8th 2020. "Kenya steps up fight against cybercrime." https://www.standardmedia.co.ke/business/sci-tech/article/2001393164/kenya-steps-up-fight-against-cybercrime.

Both the state and non-state actors need to raise more public concerns on Security and privacy matters. This is intended to ensure that each individual protects their data. There is a need to take more steps to protect their privacy online, manage Security on their electronic devices, and teach the young people about the risk of posting certain information online and interacting with strangers online. [223]The public needs to be made aware of the shift in technology platforms and the new ways cybercriminals use in targeting them. The public needs to be conversant with the new forms of technical exploitation of operating systems and how cybercriminals make them an easy target. The awareness programs will need to include information such as the need to adopt new secure systems.

5.8 Regional recommendations on fighting cyber crime

The governments within the African region need to accelerate the ratification and implementation of the Au Convention on cybersecurity and personal data protection. This will prove their seriousness and commitment to fighting cybersecurity threats. There is also a need for them to develop a national strategy on cybersecurity and operational action plan, which will be vital in combating cyber terrorism. Countries such as Kenya and Zambia, through the legislation, need to draft and review more cyber legislation, to criminalize the offenses related to the illicit use of ICT. They will also need to create national Computer Emergency Readiness Teams (CERTs), which will be mandated with monitoring networks and exchanging best practices that can help in effected collaboration.[224] Another recommendation to the state actors within developing nations is

[223]National Cybersecurity Strategy. 2014. Ministry of Information Communications andTechnology.http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf.

[224] Ibid

to develop legal and institutional frameworks that will be for personal data protection. This is in addition to establishing a national protection authority.

Both state and non-state actors can work together to develop a robust culture of cybersecurity, which will work towards recognizing and responding to the global threats and challenges that are associated with the internet, mobile networks, and many other related technologies. Together, they can work in the development of diplomacy abilities, by taking part in the discussions carried out at international levels such as the UN. The state actors need to establish regional cybersecurity centers, where they will aim to serve as catalysts to enhance regional cooperation, collaboration, and coordination, as a way of addressing the escalating cyber threats. [225]The governments across regions, such as East Africa, will need to develop Regional Computer Emergency/ Incident Response Teams (CERTs /CIRTs), which will aid in the promotion of formal and informal exchange of information among the involved nations. At the continental level, there will also be a need for a harmonized approach, which will help in creating a secure, robust, and resilient cyber environment across the continent. [226] They also will need to undertake more dialogues, through conventions and workshops where they can share ideas on the best initiatives to undertake a way of ensuring that sustainable cybersecurity measures are in place.

5.9 Conclusion

Multiple studies expound on the issue of cybersecurity. Nevertheless, it should be understood that the rise of cybersecurity has emerged as a result of the growth in modern technology. The internet is no longer about sending mail or compiling information, but rather

[225]Community Authority of Kenya. (2019). *Cybersecurity meeting calls for expedition of Data Protection Bill and investments in more professionals.* Retrieved from https://ca.go.ke/cybersecurity-meeting-calls-for-expedition-of-data-protection-bill-and-investments-in-more-professionals/

[226] Ibid

handling anything including electrical plants and household items. As much as the internet has had its upside with many advantages to businesses and institutions, it has also come with more disadvantages, which ought to be addressed by the various stakeholders, including both the government and non-government agencies. Despite the many advantages associated with the growth of modern technology and the use of the internet, the downside of the development has been the rise of cyber insecurity, where it is presently easy to access people's personal information and data and use it illegally for personal benefits. There has been an increased fear over cybersecurity since people are worried about the comprise of privacy notions, where it is easier for people to survey others easily, infringe their privacy, and even acquire data illegally. It has become more common for people at the office, home, and even at the government level to be allowed surveillance and internet filtering, which compromises people's security and privacy.

From the study, it is therefore apparent that there is a need for a major collaboration between the state and non-state actors. In both Kenya and Zambia, which are both developing nations, both the state and non-state actors have a critical role in ensuring that the fight against cyber threat is a success. It is apparent that despite the measures in place by both state and non-state actors, more needs to be done to ensure that the two agencies are ready to deal with increasing forms of cyber threats. It is also manifest, that there will be a need for further studies on the sustainable solutions towards war on cyber threats.

References

Ajayi, E. 2016. "Challenges to enforcement of cyber-crimes laws." Journal of Internet and Information 6 (1): 1-12.

Amazouz, Souhila. 2019. "International Cyber Security Diplomatic Negotiations: Role of Africa in Inter-Regional Cooperation for a Global Approach on the Security and Stability of Cyberspace."

Anderson, Ross, Chris Barton, Rainer Bölme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. "Measuring the changing cost of cybercrime." (2019).

Aspers, Patrik, and Ugo Corte. "What is qualitative in qualitative research?" Qualitative Sociology 42, no. 2 (2019): 139-160.

Ball, Helen L. "Conducting online surveys." Journal of Human Lactation 35, no. 3 (2019): 413-417.

Boes, Sanne, and E. Rutger Leukfeldt. "Fighting cybercrime: A joint effort." In *Cyber-physical security*, pp. 185-203. Springer, Cham, 2017.

Brunner, M. (2014). Challenges and Opportunities in State and Local Cybercrime Enforcement. JOURNAL OF NATIONAL SECURITY LAW & POLICY, 10, 563-583.

BSA Global Software Survey. (June 2018). Software Management: Security Imperative, Business Opportunity. Retrieved from https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf

Business Daily Africa. NOVEMBER 19, 2012. "Kenya steps up fight against cyber crime." https://www.businessdailyafrica.com/bd/corporate/companies/kenya-steps-up-fight-against-cyber-crime-2019556.

Caravelli, Jack, and Nigel Jones. 2019. Cyber Security: Threats and Responses for Government and Business. Praeger Security International.

Careers in cyber security. 2019. Cyber Security and Its Role in Government. How Government Can Combat Cyber Threats. https://careersincybersecurity.com/cyber-security-and-its-role-in-government/.

CHAWE, MICHAEL. 2018. Zambia opposition MPs reject move to introduce new cyber laws. https://www.theeastafrican.co.ke/tea/rest-of-africa/zambia-opposition-mps-reject-move-to-introduce-new-cyber-laws-1397652.

Chetty, R.-L. (2018). Kaspersky Lab report says South Africans most susceptible to online banking attacks. Retrieved from https://www.htxt.co.za/2018/11/12/kaspersky-lab-report-says-south-africans-most-susceptible-to-online-banking-attacks/

Chisenga, Sydney. April, 2020. Zambia - Data Protection Overview. https://www.dataguidance.com/notes/zambia-data-protection-overview.

Citizen TV. (2018). Ksh.5M fine or 2 years in jail for fake news as Uhuru signs Cyber-Crimes Bill. Retrieved from https://citizentv.co.ke/news/ksh-5m-fine-or-2-years-in-jail-for-fake-news-as-uhuru-signs-cyber-crimes-bill-200524/

Clark-Kazak, Christina. "Developing ethical guidelines for research" Forced Migration Review 61 (2019): 12-13.

Community Authority of Kenya. 2019. Cybersecurity meeting calls for expedition of Data Protection Bill and investments in more professionals. https://ca.go.ke/cybersecurity-meeting-calls-for-expedition-of-data-protection-bill-and-investments-in-more-professionals/.

Connelly, Lynne M. "Trustworthiness in qualitative research." Medsurg Nursing 25, no. 6 (2016): 435-437.

Davies, Gemma. "Court of Appeal High Court: Extradition, forum bar and concurrent jurisdiction: Is the case of Love a precedent for trying hackers in the UK? Lauri Love v (1) The Government of the United States of America (2) Liberty [2018] EWHC 172." *The Journal of Criminal Law* 82, no. 4 (2018): 296-300.

Eggers, W. (2016). Government's Cyber Challenge. Deloitte Review.

Eilstrup-Sangiovanni, M. 2018. "Why the World Needs an International Cyberwar Convention." Philos. Technol 31, 379–407. doi: https://doi.org/10.1007/s13347-017-0271-5.

European Police Science and Research Bulletin · Special Conference Issue Nr. 2. Germany.

Europol, & Eurojust. (2019). Common challenges in combating cybercrime. Europol and Eurojust Public Information.

EUROPOL. 2011. The Changing Face of Cybercrime. https://www.europol.europa.eu/newsroom/news/changing-face-of-cybercrime.

Evans, Caleb. "The Legality and Considerations of Countering International Terrorism." *Oklahoma City University's Undergraduate Research Journal*: 73.

Evans, Joel R., and Anil Mathur. "The value of online surveys: A look back and a look ahead." Internet Research (2018).

Eweniyi, Odunayo. 2014. "Kenyan Government Joins the Fight Against Cybercrime." https://techcabal.com/2014/05/07/kenyan-government-joins-fight-cybercrime/.

Federal Bureau of Investigation. 2017. "Roles and Responsibilities for Defending the Nation from Cyber Attack." https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities.

Felson, Marcus, Martin A Andresen, and Graham Farrell. 2015. The Criminal Act. Palgrave Macmillan.

Gercke, Marco, Tatiana Tropina, and Christine Sund. 2010. "THE ROLE OF ICT REGULATION IN ADDRESSING OFFENSES IN CYBERSPACE."

Gilligan, J. M. (2017). The Government Role in Improving Cyber Security. Retrieved from https://www.globalcyberalliance.org/the-government-role-in-improving-cyber-security/

Hanyama, Nchimunya, and Dani Banda. 2017. Policies and Legislation for Internet Access and Usage in Zambia. http://article.sapub.org/10.5923.j.scit.20170703.02.html.

ICT Policy Africa. 2009. The Electronic Communications and Transactions Act, 2009. https://ictpolicyafrica.org/en/document/fujb45s0qsb?page=3.

Ismail, Nick. 29 January 2018. "Collaboration is key in fighting cybercrime." https://www.information-age.com/collaboration-key-fighting-cybercrime-123470569/.

Ismail, Nick. 29 January, 2018. "Collaboration is key in fighting cybercrime." https://www.information-age.com/collaboration-key-fighting-cybercrime-123470569/.

Jakobi, A. P. Non-State Actors All Around: The Governance of Cybercrime. (2013): 129-148. doi:https://doi.org/10.1057/9781137334428_7

Jakobi, A., & Wolf, K. (2013). Non-State Actors All Around: The Governance of Cybercrime. The Transnational Governance of Violence and Crime. Governance and Limited Statehood. doi:https://doi.org/10.1057/9781137334428_7

Jakobi, Anja P. 2013. "Non-State Actors All Around: The Governance of Cybercrime." 129-148. doi: https://doi.org/10.1057/9781137334428_7.

KENYA GAZETTE SUPPLEMENT. 2018. The Computer Misuse and Cybercrimes Act, 2018. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf.

Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International Journal of Critical Infrastructure Protection* 25 (2019): 36-49.

Korir, Cheruiyot. November 29, 2016. "Government to curb cyber crimes." https://ict.go.ke/government-to-curb-cyber-crimes/.

KPMG. 2011. "Issues Monitor." Cyber Crime –A Growing Challenge for Governments. https://institutes.kpmg.us/content/dam/institutes/en/government/pdfs/2011/cyber-crime-growing-challenge.pdf.

Kshetri, N. (April 2019). Cybercrime and Cybersecurity in Africa. doi:https://doi.org/10.1080/1097198X.2019.1603527'

Kshetri, N. 2013. "Cybercrime and Cybersecurity in Sub-Saharan African Economies. In: Cybercrime and Cybersecurity in the Global South." In International Political Economy, 152-170. London: Palgrave Macmillan.

Kshetri, Nir. "Cybercrime and cybersecurity in Africa." (2019): 77-81.

Lee, Laura. "Cybercrime has evolved: it's time cyber security did too." *Computer Fraud & Security* 2019, no. 6 (2019): 8-11.

Lewis, James A. "Sovereignty and the Role of Government in Cyberspace." Brown J. World Aff. 16 (2009): 55.

London Institute of Banking & Finance. 2017. "The changing face of Cybercrime." A special report by The London Institute of Banking & Finance. https://www.libf.ac.uk/docs/default-source/default-document-library/the-changing-face-of-cybercrime464f2e43ec86691782d0ff00001f97d9.pdf?sfvrsn=53c9478d_0.

Lovet, G. (2009) Fighting Cybercrime: Technical, Juridical and ethical Challenges, Virus Bulletin Conference, September 2009. available at: http://www.fortiguard.com/papers/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf

Luknar, Ivana M. "Cybercrime-Emerging Issue." *Archibald Reiss Days* 10 (2020).

MENA, CHALLENGES AND LEGAL RESPONSE." http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

Nadir, I., and T. Bakhshi. 2018. "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. In 2018 International Conference on Computing, Mathematics and Engineering Technologies." 1-7.

Nanyun, Nankpan, Nasiri, and Alireza. 2020. "Role of FATF on financial systems of countries: successes and challenges." Journal of Money Laundering Control 1.

Naqvi, Syed. "Challenges of cryptocurrencies forensics: a case study of investigating, evidencing and prosecuting organised cybercriminals." In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1-5. 2018.

National Cybersecurity Strategy. 2014. Ministry of Information Communications and Technology. http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf.

Nayak, M. S. D. P., and K. A. Narayan. "Strengths and weakness of online surveys." IOSR Journal of Humanities and Social Science 24, no. 5 (2019): 31-38.

Nchimunya, Hanyama, and Dani Banda. 2017. "Policies and Legislation for Internet Access and Usage in Zambia." Science and Technology (Scientific Academic Publishing) 7 (3): 72-78.

Ndeda, Laureen Akumu, and Collins Otieno Odoyo. "CYBER THREATS AND CYBER SECURITY IN THE KENYAN BUSINESS CONTEXT." (2019).

News24. 2004. Zambia to delete cyber crime. https://www.news24.com/news24/zambia-to-delete-cyber-crime-20040729.

Nikkel, Von Bruce. 2018. "Positive Changes and Collaboration in the Fight Against Cybercrime." https://www.societybyte.swiss/en/2018/01/22/positive-changes-and-collaboration-in-the-fight-against-cybercrime/.

Nir, Kshteri. 2019. "Cybercrime and Cybersecurity in Africa." Journal of Global Information Technology Management 22 (2): 77-81.

Njoroge, George M. "Human Factors Affecting Favourable Cybersecurity Culture-a Case of Small and Medium-sized Enterprises Smes Providing Enterprise-Wide Information Systems Solutions in Nairobi City County in Kenya." PhD diss., University of Nairobi, 2020.

Nouh, Mariam, Jason RC Nurse, Helena Webb, and Michael Goldsmith. "Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement." *arXiv preprint arXiv:1902.06961* (2019).

Nuredini, A. (2014, August). CHALLENGES IN COMBATING THE CYBERCRIME. Mediterranean Journal of Social Sciences, 5(19), 592-600.

OBURA, FREDRICK. November 8th 2020. "Kenya steps up fight against cybercrime." https://www.standardmedia.co.ke/business/sci-tech/article/2001393164/kenya-steps-up-fight-against-cybercrime.

Quarshie, Henry Osborn, and Alexander Martin-Odoom. 2012. "Fighting Cybercrime in Africa." 2(6): 98-100. doi:10.5923/j.computer.20120206.03.

Rice, Stephen, Scott R. Winter, Shawn Doherty, and Mattie Milner "Advantages and disadvantages of using internet-based survey methods in aviation-related research." Journal of Aviation Technology and Engineering 7, no. 1 (2017): 5.

SAMBULI, NANJIRA, JULIET MAINA, and TYRUS KAMAU. 2016. "Mapping the Cyber Policy Landscape: Kenya." https://www.gp-digital.org/wp-content/uploads/2016/12/Kenya-Cyber-Policy-Mapping-final-i-1.pdf.

Savage, Ed. 2019. "Tackling the challenges of cyber security." https://www.paconsulting.com/insights/tackling-the-challenges-of-cyber-security-the-role-of-government/.

SERIANU. 2017. "Africa Cyber Security Report 2017." Demystifying Africa Cyber Security Poverty Line. https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf.

Sharma, Gaganpreet. "Pros and cons of different sampling techniques." International journal of applied research 3, no. 7 (2017): 749-752.

Sigholm, J. (2013). Non-state actors in cyberspace operations. Journal of Military Studies, 4(1), 1-37.

Sigholm, Johan. 2016. "Non-State Actors in Cyberspace Operations." Swedish National Defence College, Sweden. doi: https://doi.org/10.1515/jms-2016-0184.

Singer, P. W., & Friedman, A. (2014). Cybersecurity And Cyberwar What Everyone Needs To Know. Oxford University Press.

Sofaer, A. D., Grove, G. D., & Wilson, G. D. Draft International Convention To Enhance Protection from Cyber Crime and Terrorism. The Transnational Dimension of Cyber Crime and Terrorism, (2001):249-265.

Sprinkel, Shannon C. "Global Internet Regulation: The Residual Effects of the ILoveYou Computer Virus and the Draft Convention on Cyber-Crime." *Suffolk Transnat'l L. Rev.* 25 (2001): 491.

Stalph, Florian. "Classifying Data Journalism: A content analysis of daily data-driven stories." Journalism Practice 12, no. 10 (2018): 1332-1350.

Stock, Jürgen, Michael Daniel, and Tal Goldstein. 2020. "Partnerships are our best weapon in the fight against cybercrime. Here's why." https://www.weforum.org/agenda/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/.

Tan, Aaron. 2017. "Collaboration is key to combating cyber crime." https://www.computerweekly.com/news/450421906/Collaboration-is-key-to-combating-cyber-crime.

Telecommunication Development Sector. September, 2012. "UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE." http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

Tereshchenko, Natalia. 2013. "US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure." https://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/.

The conversation. December, 2019. "What's been done to fight cybercrime in East Africa." https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240.

The National KE-CIRT/CC. 2012. Cybersecurity: past, present and future. https://www.ke-cirt.go.ke/index.php/cybersecurity-past-present-and-future/.

The Parliament of Zambia. 2004. The Zambia Computer Misuse and crimes Act, 2004. https://ictpolicyafrica.org/en/document/0vodshuq3cj?page=4&raw=true.

Tropina, Tatiana. 2009. "Cyber-policing: the role of the police in fighting cybercrime." European Police Science and Research Bulletin · Special Conference Issue Nr. 2. Germany.

Union, African. "A global approach on Cybersecurity and Cybercrime in Africa." (2015).

United Nations. 2020. "Government Support: Zambia." UN: Victims of Terrorism Support Portal. https://www.un.org/victimsofterrorism/en.

van der Meer, Sico. "How states could respond to non-state cyber-attackers." (2020).

Wall, David S., and Matthew L. Williams. "Policing cybercrime: networked and social media technologies and the challenges for policing." (2013): 409-412.

Xinhua. 2020. "Kenya to partner with private sector to boost cyber seurity." http://www.xinhuanet.com/english/2020-11/06/c_139496641.htm.

Young, S. T., and K. K. Dhanda. "Chapter 9: Role of governments and non-governmental organizations." Sustainability: Essentials for Business; SAGE Publications, Inc.: Thousand Oaks, CA, USA (2013).

Appendix

Questionnaires

i. What is the current state of international Inter-agency coordination amongst all the relevant actors in finding a sustainable solution to the threat of cybercrime?

ii. How can the state and non-state actors collaborate to fight against cybercrimes and ensure sustainable cybersecurity in their respective nations?

iii. What is the current state of collaboration between government and non-state actors, and how effective is the collaboration in the fight against cybercrime?

iv. What measures should be taken by the government and other non-state actors to ensure that there are constant structures in place to fight with the increasing cases of cybercrimes?

v. What are the different strategies that the Kenyan and Zambian state and non-state actors have to protect the institutions and the citizens in their respective countries?

vi. Is there any international collaboration amongst these nations that can help develop effective cybersecurity solutions?

vii. How often do the relevant security authorities from state and non-state actors meet to discuss on their level of preparedness when it comes to cybersecurity?

viii. Do the staff and employees of both state and non-state actors in both countries provide or leak confidential information on cyber security without proper authorization?

ix. How often do the trainings and updates of cybersecurity matters take place?

x. Do the employees in the security agencies leak or disclose sensitive information with non-employees while away from work?

xi. Are the old storage gadgets such as hard drives and flash disks destroyed with the content they carry in?

xii. Are users in both state and non-state actors trained to recognize a legitimate warning message from a scam message that could result in downloading a virus?

xiii. Do both countries have their back up data storage devices encrypted?

xiv. When was the last time both countries conducted and documented an independent information security risk assessment?

xv. Have both countries tried and tested the incident response plan with clearly assigned responsibilities?