

UNIVERSITY OF NAIROBI

INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES

**A CRITICAL ANALYSIS OF THE CHALLENGES FACING COUNTER-
CYBERCRIME IN 21ST CENTURY AFRICA: A FOCUSED COMPARISON OF
KENYA AND RWANDA**

BERNARD BARASA WALUMOLI

R50/35343/2019

SUPERVISOR: DR MUMO NZAU

**A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE AWARD OF MASTER OF ARTS IN INTERNATIONAL
STUDIES**

NOVEMBER 2021

DECLARATION

I declare that this is my original work and has not been presented for academic award or qualification in any institution of higher learning. In addition, appropriate referencing has been made where concerned.

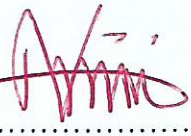
Signature:  Date: 3/12/2021

Bernard Barasa Walumoli

Reg.No. R50/35343/2019

Supervisor

This research has been submitted for examination with my approval as the assigned university supervisor.

Signature:  Date: 03/12/21

Dr. Mumo Nzau

ACKNOWLEDGMENT

First, I would like to thank the almighty God for seeing me through National Defense College course number 22 of 2019/2020 in the wake of Covid 19. I also wish to extend my sincere gratitude to the Director directorate of criminal investigations Mr. George Kinoti, CBS, for granting me an opportunity to study, and for paying my fees. I also wish to extend my appreciation to Dr. Mumo Nzau for his professional, experienced and scholarly guidance. Mr. Wamagata Kairu, Mr. Titus Macharia and Col. Franco Rutagengwa (Rwanda) all of NDC Course 22 for their technical support. My wife Ann Masete and our children Purity, J Brian, Faith and Maxvier for encouraging me and being understanding when I dedicated more attention to my studies at their expense. May I also register my sincere appreciation to the National Defense College leadership and faculty for their enthusiasm to mold and shape me into a strategic leader and for the willpower they demonstrated to see to it that the course is completed within the set timelines despite the challenges posed by Covid-19 pandemic.

LIST OF ABBREVIATIONS

AU	African Union
AUC	Africa Union Commission
CAK	Communication Authority of Kenya
CBN	The Central Bank of Nigeria
CD ROM	Compact Disc Read-Only Memory,
CECC	Council of Europe's Convention on Cyber Crime
CISO	Cyber and Information Security Officer
Covid 19	Coronavirus
DCI	Directorate of Criminal Investigation
EC3	European Cybercrime Centre
ECOWAS	Economic Community of West African States
ECT	Electronic Communications and Transactions
ERA	Academy of European Law
EUROPOL	European Police
FBI	Federal Bureau of Investigation
GB	Giga Bites
GCI	Global Cyber Security Index
GoK	Government of Kenya
HP	Hewlett-Packard computer soft wear
IC3	Command Control and Communication
ICT	Information Communication and Technology
INTERPOL	International Police
IOCTA	Internet Organized Crime Threat Assessment
IoT	Internet of Things
IP	Internet Protocol
ISC	Internet Security Center
ISPS	Internet Service Providers
IT	Information Technology
ITU	International Telecommunication Union
KE-CIRT/CC	Kenya Computer Incident Response Team Coordination Center

LSK	Law Society of Kenya
MLAA	Mutual Legal Assistance Agreements
MLATs	Mutual Legal Assistance Treaties
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NCPF	National Cyber Security Policy Framework
NGOs	Non-Governmental Organizations
ODPP	Office of the Director of Public Prosecutions
PKI	Public Key Infrastructure
RAM	Random Access Memory
RECs	Regional Economic Communities
Rw-CSIRT	Rwanda Computer Security and Incident Response Team
SAPS	South African Police Service
SIM	Subscriber Identification Module
Tor	The Onion Router
UK	United Kingdom
UN	United Nations
UNGGE	United Nations Group of Governmental Experts
US	United States
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Networks
WWW	World Wide Web

ABSTRACT

This study endeavored to explore the challenges facing counter cybercrime in the 21st Century Africa by having a focused comparison of Kenya and Rwanda. Rwanda was picked on because she is doing better than Kenya in addressing these challenges. Counter cybercrime challenges have increased globally, regionally and even locally despite the efforts put in place to address this challenge. Given the serious nature of cybercrime, its international nature and implications it is evident that there is dire need for a common understanding of such challenges internationally, regionally and locally in order to deal with the challenge more effectively. This challenge needs global legislation and cooperation by all states; however as at now there is no such an effective legislation while cooperation is based on bilateral and multilateral relations among willing countries. Findings from other related studies indicate that counter cybercrime challenges in Africa and specifically in Kenya have kept on escalating making it difficult to investigate, prosecute and convict the perpetrators. This study aimed at revealing the existing gaps in addressing counter cybercrime in Africa and Kenya in particular. And suggest more effective ways of dealing with the identified challenges by borrowing from more successful countries internationally and Rwanda in particular. This study looked at the challenges affecting counter cybercrime both internationally and locally, and showing the extent to which international cooperation, initiatives and policies have succeeded in different jurisdictions. The ultimate objective here is to identify areas where improvement is needed. As part of the recommendations this study suggests that it is necessary to establish a universally recognized law that will apply equally internationally. In order to deal with various hazards posed by cybercriminals, this study recommends that parliament pass more rigorous and punitive regulations compared to the existing ones. A deliberate national education and awareness campaign on the impact of cybercrime is critical in lowering the country's cybercrime rates.

TABLE OF CONTENTS

DECLARATION	ii
ACKNOWLEDGMENT	iii
LIST OF ABBREVIATIONS	iv
ABSTRACT	vi
TABLE OF CONTENTS	vii
LIST OF FIGURES	xi
LIST OF TABLES	xii
CHAPTER ONE:INTRODUCTION	1
1.1 Background of the Problem	1
1.2 Problem Statement	5
1.3 Research Objectives	5
1.3.1 Research Questions	6
1.4 Literature Review.....	6
1.4.1 On the Challenges Facing Counter-Cybercrime at the Global Level	6
1.4.2 On the Challenges Facing Counter-Cybercrime Efforts in Africa.....	9
1.4.3 Challenges affecting Counter Cybercrime Processes in Rwanda and Kenya...	11
1.4.3.1 Rwanda	11
1.4.3.2 Kenya	12
1.4.4 Research Gaps.....	13
1.5 Justification of the Study	13
1.6 Theoretical Framework.....	15
1.7 Hypotheses	17
1.8 Research Methodology	17
1.8.1 Study Design	17
1.8.2 Sampling Procedure	18
1.8.3 Methods of Data Collection	18
1.8.4 Analysis of Data.....	20
1.9 Scope and Limitation	20
1.10 Chapter Outline.....	21

CHAPTER TWO:CHALLENGES FACING COUNTER-CYBERCRIME AT GLOBAL LEVEL: AN ASSESSMENT	22
2.1 Challenges Facing Counter-Cybercrime at Global Level: An Assessment	22
2.2 Inadequate Legislation	22
2.3 Law Enforcement Challenges	24
2.4 The Question of Jurisdiction	25
2.5 Counter Cybercrime Challenge of Extradition	26
2.6 Ineffective Reporting and Shortage of Cybercrime Data	27
2.7 Identity of Cybercriminals	29
2.8 Nature of Evidence	30
2.9 The Cost and Time Factor in Investigations and Prosecution	31
2.10 Issue of Training and Poor Remuneration for Law Enforcement Agencies	31
2.11 Loss of Cybercrime Data	32
2.12 The Challenge of New and Emerging Technologies	32
CHAPTER THREE:CHALLENGES OF COUNTER-CYBERCRIME EFFORTS IN AFRICA.....	34
3.1 Challenges of Counter-Cybercrime Efforts in Africa.....	34
3.2 Challenge of Jurisdiction	35
3.3 Challenges of Cybercrime Legislation.....	38
3.4 Evidential Challenge	40
3.5 Challenges of Extradition	42
3.6 Challenges of Dual Criminality	43
3.7 Challenges of legal and International Cooperation.....	44
3.8 Challenges of Anonymity of Criminals	45
3.9 Challenge of Reliance on Information and Communication Technologies	46
3.10 Challenge of Readily Available Devices and Ease Access	47
3.11 Challenge of Availability of Information	47
3.12 Challenge of Missing Mechanism of Control of the Internet	48
3.13 Challenge of Encryption Technology	48
3.14 Drafting National Criminal Laws Challenge	50

CHAPTER FOUR: DATA PRESENTATION, ANALYSIS AND

DISCUSSION Error! Bookmark not defined.

4.1 Challenges Affecting Counter-Cybercrime Processes in Kenya and Rwanda: A

Critical Comparison 51

4.2 Counter Cybercrime Challenges Facing Kenya..... 51

4.2.1 Challenges of Legislation 53

4.2.2 Interested Parties Challenge..... 54

4.2.3 Challenge of Jurisdiction 55

4.2.4 Challenge of Extradition Processes 56

4.2.5 Challenge of Lack of Awareness of Cybercrime..... 58

4.2.6 Challenge of Anonymity of Criminals..... 59

4.2.7 Challenges of Investigation and Prosecutions 60

4.2.8 Challenges of Cooperation..... 62

4.2.9 Challenges of Costs and Time 64

4.2.10 Challenges of Current Policies..... 64

4.2.11 Challenge of Dynamic Sophistication 66

4.2.12 Challenge of Changing Cyber Technology..... 67

4.2.13 Challenge of Inadequate Training of Law Enforcers..... 67

4.3 Counter Cybercrime Challenges Facing Rwanda 68

4.3.1 Challenges of Legislation 69

4.3.2 Challenges of Jurisdiction..... 70

4.3.3 Challenges of Cyber Security and Information Awareness 71

4.3.4 Challenges of Expertise and Skills in Cybercrime Investigations 71

4.3.5 Challenges of Locating and Identifying Perpetrators 72

4.3.6 Challenges of Dynamic Technology..... 73

4.4 Secondary Data Analysis 73

4.4.1 Kenyan Approach to Counter Cybercrime 73

4.4.2 Rwanda's Approach to Counter Cybercrime..... 77

4.5 Analysis of Primary Data..... 79

CHAPTER FIVE:SUMMARY, CONCLUSION AND RECOMMENDATIONS 100

5.1 Summary, Conclusion and Recommendations 100

5.2 Summary of the Study	100
5.3 Summary of the Findings	101
5.4 Conclusions	104
5.5 Recommendations	106
5.6 Suggestions for Further Research	108
BIBLIOGRAPHY	109
APPENDICES	119
Appendix A: Questionnaire	119
Appendix B: Interview/Questionnaire Guide for Respondents.....	121

LIST OF FIGURES

Figure 4.1: The number of cyber threats detected in Kenya more than doubled to 26.6 million in the period April to June	52
Figure 4.2: Methods and implementation to combat cyber-crimes in Rwanda, February 2019.....	77
Figure 4.3: Gender presentation.....	80
Figure 4.4: Position held/ designation	81
Figure 4.5: Level of education acquired by respondents	82
Figure 4.6: Length of service of respondents.....	82
Figure 4.7: Some of the main challenges in countering cybercrime.....	84
Figure 4.8: Opinions on difference in jurisdiction and countering cybercrime	85
Figure 4.9: Legislations in countering cybercrime	86
Figure 4.10: Difficult in identifying cybercrime criminals.....	87
Figure 4.11: Training of law enforcers	88
Figure 4.12: Current criminal laws and regulations coverage of cybercrime	91
Figure 4.13: Enforcement of cybercrime laws and regulations	92
Figure 4.14: Uniformity of counter cybercrime laws	93
Figure 4.15: Opinions on total legal and international cooperation in countering cybercrime.....	95
Figure 4.16: Covering o cybercrime by National criminal laws.....	97
Figure 4.17: Mechanisms of monitoring and regulating the internet.....	98

LIST OF TABLES

Table 4.1: Response rate 83

Table 4.2 Respondents opinion on whether counter cybercrime face challenges 84

Table 4.3: Opinions on level of enforcement mechanisms..... 87

Table 4.4: Difficult in collecting cybercrime evidence 88

Table 4.5: Remuneration of law enforcers..... 89

Table 4.6: Cooperation between different countries..... 90

Table 4.7: The effect of high speed of data exchange on cybercrime investigations 94

Table 4.8: Extradition as a challenge in countering cybercrime..... 96

Table 4.9: Readily available information on the internet as a challenge in counter
cybercrime..... 97

CHAPTER ONE

INTRODUCTION

1.1 Background of the Problem

Cyber-crime is a relatively new form of crime compared to traditional crime, and it has the potential to wreak far more harm to society than other forms of crime. As a result, it has been the focus of international attention. This is for the reason that people in the whole world, be it private or public, are subject to cybercrime challenges, and it is nearly unavoidable because the entire world is now in the information age.¹ Unlike the previous centuries, the twenty-first century has been characterized by an increasingly globalized world, where criminals increasingly rely on the internet and more advanced technologies to carry out their criminal activities. This has contributed immensely to the widespread of computer related crimes around the world. Now it is ease of access to commit cybercriminal activities beyond one's borders than before, which makes this an international concern.² Just like conventional crimes, cybercrime appears in different forms and take place in a wide variety of situations and atmosphere.

Despite its notoriety, scholars and practitioners have not agreed on any one universal definition of cybercrime. Currently, there is no single universally acknowledged definition of the term cybercrime, though it is often characterized as any illegal activity involving the use of a computer as an instrument, a goal, or both, that jeopardizes a country's safety

¹ Ajayi, E. F. G. Challenges to enforcement of cyber-crimes laws and policy, Journal of Internet and Information Systems, School of Law, Kenyatta University, Nairobi, Kenya. 25 July, 2016

²Jobel Kyle P. Vecino United by Necessity, The Cyber Defense Review, Special Edition: International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2018: Cyber Conflict during Competition (2019), pp. 123-144 Published by: Army Cyber Institute Stable URL: <https://www.jstor.org/stable/10.2307/26846124>. This content downloaded from 62.24.102.106 on Fri, 17 Jan 2020 18:20:39 UTC

and economic sector.³ Simply described, it refers to any illicit activity carried out with the use of computer technology or software. Computer crime, often known as cybercrime, is regularly performed via the Internet on accessible Web-based systems.

Almost everyone who uses a computer or Internet network, including people, corporations, organizations, governments, multinationals, and internationals, uses the phrase "cybercrime." The level of attention paid to cybercrime is justified because it is partly owing to the fact that communications over the Internet is the sole medium via which all types of international trade and commerce, as well as communal contact, are performed on a daily basis.

The start of the twenty-first century ushered in a new era of transformational information, which has changed the global marketplace. Transnational criminal networks have also profited from the revolt, using it to infiltrate economies and governmental structures all around the world.⁴ The phenomenal rise has had perplexing implications for state stability and development, as well as posing a major threat to the lives and well-being of people all over the world. Due to the ever-changing Internet environment, systematized cybercrime clusters, and new 'smart' computer programs, the appearance and commission of cybercrime has taken on a new angle in recent years. New forms of illegal behavior have emerged as a result of the spread of new talents and the expansion of the Internet network.

³Kirwan, D (2017), An Investigation of the Attitudes and Environmental factors that make people more willing to participate in online crimes, Masters Dissertation, Dublin Institute of Technology

⁴Journal of International Affairs, Vol. 66, No. 1, Transnational Organized Crime (Fall/Winter 2012), pp. vii-ix Published by: Journal of International Affairs Editorial Board Stable URL: <https://www.jstor.org/stable/24388246> Accessed: 26-01-2020 12:13 UTC

Indeed, the world has transformed dramatically to become a global village; previously thought to be flat, it was then thought to be round, and now it is thought to be global and digitalized! This Trans global digital connectivity between individuals, economies, and governments has far-reaching implications.⁵ In all social areas of life, modern society is confronted with severe activities of technical and high-tech development, which are linked to rapid expansion of information knowledge and computerization of job accomplishments. On the one hand, this kind of progress in the contemporary social order has brought a plethora of conveniences; on the other hand, there is a visible presence of cautious abuse of hi-tech accomplishment, which has generated a number of snags and threats for too many personalities and throngs in society generally, and particularly in terms of national security.⁶ The globe is currently coping with these new advanced technology, crimes, victimization tactics, and new intergovernmental action avenues to compensate global impacts. The rapid pace of technology advancement continues to offer new issues that were previously unknown or underestimated.⁷

Counter-cybercrime is a global concern, and no single government can claim to be impregnable. In recent years, Africa has seen a significant increase in Internet coverage, as well as an increase in illegal cyber activities, necessitating increased energies

⁵cybercrime theory and discerning if there is a crime: the case of digital piracy Author(s): Frances P Bernat and David Makin Source: International Review of Modern Sociology, Vol. 40, No. 2 (Autumn 2014), pp. 991-19 Published by: International Journals Stable URL: <https://www.jstor.org/stable/43499904> Accessed: 18-01-2020 09:44 UTC

⁶ Mr. SC Ahmet Nuredini, PhD Candidate Professor in ISPE College, Challenges in Combating the Cybercrime, Mediterranean Journal of Social Sciences, Volume 5 No 19 August 2014, MCSER Publishing, Rome-Italy ahmetnuredini1@gmail.com

⁷Clough, J. 2015, Principles of cybercrime, Second edition, Cambridge University Press,

throughout the region to reinforce the information setup, teach users on security consciousness, and improve counter-cybercrime strategies. To understand the differences in cybercrime challenges in Africa as compared to different areas of the biosphere, one must look at the current state of information on safety in Africa, which is heavily influenced by factors such as user growth, low security awareness, insufficient training for law enforcement officers, and poor enforcement of existing laws and regulations. As communities all around the world cling to information know-how for smooth provision of services, there are those in the social order who are continually looking for ways to abuse that same technology for their own selfish criminal goals. Criminals use the Internet and other available networks as a front for their criminal activities.

As a result, as technology advances, cyber-attacks become more and more complex, amplifying the effects of cybercrime.⁸ To handle the threat of rapid rise in cyber security concerns, a strong framework is required. There has been a tremendous loss of crucial data and financial assets as a result of weak or non-existent cyber security measures. There is no single point of control for the Internet configuration.⁹ As a result, anyone with access to the internet can engage in either legal or illegal activity. Cybercriminals gain from the Internet's disorganized character. In Kenya, successful cyber-attacks are ascribed to a lack of competence to apply existing cybercrime legislation, as well as inadequate and ineffective detection tools.

⁸ Poonia, A. S. (2014), Cyber Crime: Challenges and its Classification, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN, 2278-6856.

⁹Peisert,S. Margulies, J, Nicol, D. M., Khurana, H & Sawall, C (2014).Designed-in Security for Cyber-Physical Systems. Security & Privacy, IEEE, 12(5), 9-12.

1.2 Problem Statement

Counter cybercrime challenges have increased globally, regionally and locally despite efforts put in place to address this problem. Counter cybercrime challenges need global legislation and cooperation by all countries, however currently there is no such an effective legislation, while cooperation is based on bilateral and multilateral relations among countries. Evidence from previous studies indicates that, counter cybercrime challenges in Africa and specifically in Kenya have escalated making it difficult to investigate, prosecute and convict cybercrime suspects. Available literature shows that Rwanda is doing better than Kenya in addressing counter cybercrime challenges. This study will reveal the gaps in addressing counter cybercrime challenges in Africa and Kenya in particular and suggest more effective ways of dealing with these challenges, by borrowing from more successful countries internationally, regionally and Rwanda.

1.3 Research Objectives

1. To assess the challenges facing counter-cybercrime at the global level
2. To critically examine the challenges facing counter-cybercrime efforts in Africa
3. To compare and contrast challenges affecting counter-cybercrime processes in Kenya and Rwanda
4. To proffer pertinent policies and strategies in managing the challenges of counter cybercrime in Kenya

1.3.1 Research Questions

1. What challenges face global counter-cybercrime efforts?
2. What factors affect efforts to counter cybercrime challenges in Africa?
3. What are the common challenges to both Kenya and Rwanda in countering cybercrime?
4. What are the pertinent policies and strategies in countering cybercrime in Kenya and Rwanda?

1.4 Literature Review

Despite ongoing remediation efforts at all levels which include global, regional, and national, the challenges of combating cybercrime continue to expand steadily. The difficulty posed by unrestricted access and engaging in cybercrime activities across one's borders makes it a global concern.¹⁰ According to a research published in the American Journal of International Law, there has been a growing worry about the hazards posed by transnational computer-related crime, or transnational computer crime, since the late 1980s.

1.4.1 On the Challenges Facing Counter-Cybercrime at the Global Level

Combating Computer Crime; An International Perspective was conducted by Alkaabi Ali Obaid. The biggest obstacles in countering cybercrime internationally, according to Alkaabi's report, are inadequate legislation, differences in jurisdictions, weak counter-

¹⁰Allison Peters and Amy Jordan, Countering the Cyber Enforcement Gap, Strengthening Global Capacity on Cybercrime, Third Way (2019) Stable URL: <https://www.jstor.org/stable/resrep20150>
Accessed: 15-02-2020 06:13

cybercrime strategies, lack of procedures, inadequate technology, and a lack of computer crime statistics.¹¹ He went on to say that there have been numerous studies on the construction of globally unified cybercrime legislation. As a result, he claims that law addressing cybercrime control measures and related offenses is constantly evolving in both developing and developed countries. "While every country in the world is connected to the internet now," Alkaabi writes, "many of countries do not have cybercrime laws, and even among those that have, the discrepancies and conflicts in the laws make it very difficult to investigate, prosecute, and punish cybercriminal behavior." According to him, establishing an internationally coordinated lawful outline for cyber-criminal actions has become a pressing international concern.

Alkaabi agreed with the United Kingdom's parliamentary science and technology committee that investigating electronic crimes, also known as cybercrimes, poses significant technical challenges. Recovery and analysis of technical equipment, hard disks, mobile phones, and other electronic devices is extremely difficult, time-consuming, and costly when conducting an investigation. Encryption is a challenge for cybercrime investigators, as it is tied to keeping up with the ever-changing technical innovations. The Metropolitan Police Service of London in the United Kingdom reported in 2007 that its specialist units were no longer able to deal with electronic-crime.¹²

¹¹ Alkaabi Ali O S, 2010, Combating Computer Crime: An International Perspective, Thesis Submitted in accordance with the regulations for Degree of Doctor of Philosophy, University of Southern Queensland.

¹² Her majesty's Inspectorate of Constabulary. Inspection Report Metropolitan Police , October 2007

In 2006, Kshetri found that local police forces in most countries were unable to deal with the worldwide dimension of cybercrime.¹³ Kshetri also mentioned that law enforcement organizations lack a cybercriminal database, which hinders their ability to solve such cybercrimes.¹⁴ And this is one of the setbacks in countering cybercrimes. In the same year, Bhesker stated that there are simply inadequate numbers of law enforcement officers with proper investigation abilities at the state level to effectively deal with the cybercrime threat.

On the same theme of cybercrime, Salil Mehraon points out that the problem with cybercrime laws is that they are shaped by the general structure of law in a centralized state with communal law courts.¹⁵ By 2010, reactive legislation and responsive recasting of existing criminal law actions to deal with offenses such as unauthorized access fraud, obscenity, child pornography, and copyright infringement dominated American efforts to combat Internet crime.¹⁶

When writing about cybercrime, Mark Galeotti pointed out that the link between cybercriminals and cyber terrorists represents one of the little-understood yet unavoidable hurdles to regulating the problem. And in many states, corruption and a lack of resources thwart police and court efforts to build a competent capacity to deal with cybercrime,

¹³ Nir Kshetri, 2006, *The Simple Economics of Cybercrime*, University of Carolina, U S A

¹⁴ Ibid

¹⁵ Salil K. Mehra, *Law and Cybercrime in the United States Today*, *The American Journal of Comparative Law*, Vol. 58, Supplement: *Welcoming the World: U. S. National Reports to the XVIIIth International Congress of Comparative Law* (2010), pp. 659-685 Published by: Oxford University Press.

¹⁶ Salil K. Mehra *Law and Cybercrime in the United States Today*, Source: *The American Journal of Comparative Law*, Vol. 58, Supplement: *Welcoming the World: U. S. National Reports to the XVIIIth International Congress of Comparative Law* (2010), pp. 659-685 Published by: Oxford University Press
Stable URL: <https://www.jstor.org/stable/20744558> Accessed: 23-01-2020 19:21 UTC

allowing offenders to enjoy cybernetic immunity.¹⁷ This is frequently accompanied with reluctance on the part of police to pursue crimes committed in other jurisdictions.

1.4.2 On the Challenges Facing Counter-Cybercrime Efforts in Africa

Akuta "Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law Policy and Practice," by Eric A. M, Ong'oa Isaac M, and Jones Chanika R, is a paper on cybercrime in Africa. Prior to the emergence of Information, Communication, and Technology (ICT), Sub-Saharan Africa (SSA) was regarded "behind" by the developed world, according to their research. As a result, the expansion of ICT was expected to open Africa as a region, connect it to the rest of the globe, and establish it as a member of the Universal community. This initiative exposed Africa to the unintended consequences of cybercrime activities. According to the three authors, the manifestations of cybercrime, as well as its far-reaching and possibly deadly capability for harm, caught most governments off guard. This is due to the inability of current laws, legislations, and institutions to keep up with the frightening rate at which cybercrime spread. Their research aimed to address the question of what support could be provided to the government and participants in the battle against cybercrime in Sub-Saharan Africa. Different governments have worked hard to put in place measures to help battle this scourge, but despite their best efforts, they have generally failed to eradicate cybercrime.

¹⁷Mark Galeotti The cyber menace, Source: The World Today, Vol. 68, No. 7 (December 2012 & January 2013), pp. 32-35 Published by: Royal Institute of International Affairs Stable URL: <https://www.jstor.org/stable/41962876> Accessed: 24-01-2020 18:43 UTC

In their research, the three academics were interested in three main topics. First, they wanted to identify the many parties involved in the battle against cybercrime in Sub-Saharan Africa. Second, the stakeholders' current laws and regulations, policies, and best practices in combating this threat were assessed. Third to address the impediments that these stakeholder organizations and institutions confront when it comes to combating cybercrime.

The three discovered during their research that cybercrime concerns are global in scope and transcend political and geographical boundaries. As a result, numerous countries in Sub-Saharan Africa have attempted to coordinate efforts within their own regions to combat cybercrime in Africa and around the world. These efforts resulted in the formation of regional blocs in Africa, such as the East Africa Community (EAC), the Central African Economic and Monetary Community (CEMAC), the Economic Community of West African States (ECOWAS), and the Southern African Development Community (SADC), to work toward harmonization of laws, holding working sessions to train law enforcement officers, and partnering with other international organizations and companies to combat cybercrime.¹⁸ The researchers concluded that nation states should retrain more skilled police officers in cybercrime-related sectors. Computer studies and issues concerning cybercrime should as well be part of the top disciplines on the curriculum of Police Academies, to equip officers with the requisite knowledge to counter cybercrime in their respective countries, regions and the world at large.

¹⁸ AkutaE.A.M, etal, Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice, Nelson Mandela School of Public Policy, Southern University Baton Rouge 3Criminal Justice Department, Southern University Baton Rouge, Accepted 05 April 2011

1.4.3 Challenges affecting Counter Cybercrime Processes in Rwanda and Kenya

1.4.3.1 Rwanda

"Cybercrimes in Rwanda: An investigative case study of pirating in Nyarugenge District from 2005 to 2010," wrote Ndayisabye Heredion. In his research, he looked into cybercrime in Rwanda and how it relates to the current computer technology flow. Ndayisabye discovered that Rwanda had high expectations in terms of Vision 2020, which aimed for Rwanda to become a technology-led economy by 2020, transforming it into a regional ICT hub. Unfortunately, as more people have access to new technologies and gain the requisite know-how, the criminal fraternity at all levels have quickly grasped cutting-edge technology. As a result, no format can be safely maintained without the use of modern technologies such as scanners and printers, Micro Soft Imaging tool, Desktop Publishing, Adobe Illustrator, Scan soft Portable Document Format professional, hard disk imaging tools, and burning software. As a result, pirate of valuable official papers, counterfeiting and falsification of monetary symbols, misappropriation of public funds, and piracy of artistic work are all on the rise.

Rwanda, he claims, is becoming more reliant on digital technologies. He suggests forming a specific interest group on computer crime, forensics, and investigation in order to mitigate dangers and capitalize on opportunities presented by technology. This would be a multi-agency taskforce made up of professionals from diverse fields of computer science, such as networking, multimedia, and forensics. Raising awareness of cybercrime among policymakers, stakeholders, and the general public increases the number of reports,

as well as the security tactics used to protect the information, such as the use of encryption and decryption procedures with tracking order numbers.

1.4.3.2 Kenya

Chebigon Kangogo conducted research on the topic of "Cybercrime in Kenya: Myth or Reality." The study's major goal was to see if the problem of cybercrime had spread to developing countries, using Kenya as a case study. One of the most obvious differences between the law and Internet use, according to his research, is the publication and consumption of banned information, as well as the use of the Internet as a channel for the illicit exploitation of intellectual property. Opportunities, a lack of guardianship, poor legislation, and extra-territorial difficulties are all significant reasons.

Kenya also lacks laws and regulations governing digital signatures and electronic contracts, according to the report. Because there are no official regulations for encryption keys to be maintained under lock and key by a government agency, and there are no size restrictions on encryption keys, importing encryption technology into the country is simple. Aside from that, Kenya is not a signatory to any encryption-related accords, and the government has no defined policy on the usage of encryption technology. According to this researcher, Kenya lacks explicit laws against computer-related crimes such as data destruction or alteration, interference with the authentic use of a computer system, theft of intangible property, and unlawful entree into a computer scheme. As a result, Kenya needs to advance its legislation to adequately safeguard electronic trade and sensitize the judiciary to allow electronic evidence to be admissible in judicial processes. According to

the findings, a comprehensive legislative framework addressing specific dangers to electronic activity and infrastructure is required. The study emphasized the need for a comprehensive anti-Cybercrime framework to protect moral standards, proprietary interests, privacy, national security integrity, and healthy foreign relations, all of which are increasingly at risk as digital technology continues to expand its influence over our day-to-day activities.

1.4.4 Research Gaps

According to the reviewed literature, several studies have been conducted on computer crime and cyber legislations, consequences of cybercrime on the economy, cybercrime prevention measures, cybercrime types, and cybercrime causes. However, not little has been done to address the issue of counter-cybercrime difficulties and counter-measures. This study is expected to spark a national conversation that will lead to the implementation and oversight of methods that will improve counter-cybercrime responsiveness at all levels and reduce counter-cybercrime problems. The study also intends to persuade Kenya to support the development and implementation of international cybercrime legislation in order to address the issue of jurisdiction in counter-cybercrime investigations and prosecutions.

1.5 Justification of the Study

The difficulty of developing rejoinder approaches and resolutions to address crimes committed through the computer is a big challenge for least developed states.¹⁹

¹⁹ Gercke, M. 2012 “Cybercrime”, Understanding Cybercrime Phenomena, Challenges and legal response, September 2012

Successfully countering cybercrime is an uphill mission that heavily relies on embracing the best practices in matters of policy and strategy, legislation, technological advancement, and adequate funding. These important aspects are lacking in Kenya yet they have enabled western countries to manage counter cybercrime challenges. Counter cybercrime challenge is an international issue that calls for collective global efforts and strategies to manage it. In western countries there are arrangements among countries on how to jointly deal with counter cybercrime challenges. However, in Africa different jurisdictions deal with counter cybercrime challenges differently, leaving room for criminals to take advantage of the gap to undermine their efforts. Rwanda is doing better than Kenya in enforcement of the laws put in place to counter cybercrime challenges as compared to Kenya.

Therefore, Kenya can borrow from Rwanda's best practices. This study has been undertaken at an appropriate time when Kenya is trying very hard to put in place serious legal and formal procedures to review counter cybercrime challenges both at the national and global echelons. This study is, thus, expected to influence national policies on counter cybercrime challenges, there by augmenting the current efforts put in place. The research will inform the policy makers' ways of cooperating with other countries; sharpen their skills further on structural, operational and tactical performance for better functioning of counter cybercrime management systems. This study aims at contributing to the existing academic literature on the counter cybercrime challenges, which will be handy to scholars, academicians and practitioners dealing with the subject matter, especially given the

dynamism of counter cybercrime challenges today. It will also inform individual citizens, corporations and businesses, who are currently facing counter cybercrime challenges.

1.6 Theoretical Framework

To better understand how cybercrime concerns can be better handled this study employed securitization theory. Securitization as a theory falls under the umbrella of critical security studies, which gained popularity in the post-Cold War era. Securitization theory was created by Copenhagen School members Barry Buzan, Ole Waever, Jaap de Wilde, and others. The Conflict and Peace Research Institute (COPRI) in Copenhagen produced the majority of the works in the 1990s. The theory of securitization is now well-established for dealing with security issues.²⁰ The strength of securitization theory is based on the fact that security is a stated word or action, and that designating anything as a "security" concern makes it real. Counter-cybercrime challenges must be classified as a security issue in this situation before they receive the attention they need.

The process by which a person, a state, or another issue becomes a matter of "Security" is referred to as securitization theory. As a result, the topic of this research is counter-cybercrime difficulties. This permits for the deployment of extraordinary methods or alternative measures in the name of security, which are preferable to political or diplomatic procedures, to handle the pertinent issues as soon as possible. In this regard, the counter-cybercrime challenge has been regarded as a critical issue that must be addressed immediately. This has been done by the actors, who are usually people in

²⁰Stritzel H. (2014) Securitization Theory and the Copenhagen School. In: Security in Translation. New Security Challenges Series. Palgrave Macmillan, London

positions of responsibility on key domestic and international issues. This increases the likelihood of a successful securitization of a given issue. The issues offered for Securitization are those that are thought to constitute an experiential risk to a referent object's well-being. The referent object in this scenario is a Nation that is ostensibly in danger and requires protection from counter-cybercrime engagements. Securitization, according to Abrahamsen, is a socially conceived security concern that gets represented and recognized as the state responds with whatever tools are available.²¹

Kenya's government has used information technology in most of its business contacts with the public, institutions, and foreign governments, making it vulnerable to cyber-attacks. This chasm must be bridged by appropriately addressing counter-cybercrime difficulties and rigorously implementing counter-cybercrime policies and methods. There is a widespread belief that Kenya's counter-cybercrime issues have hampered investigations and prosecutions of cybercrime in Kenya and Africa as a whole. This trend has resulted in cybercriminals getting away with more crimes, posing a threat to the government, businesses, and individuals. Overall, the idea of securitization is particularly relevant in our study since the risk of counter-cybercrime is empirical and requires immediate government involvement.²²

²¹Abraham, D. *The Best Defense? Legitimacy and Preventive Force*, Stanford, CA: Hoover Institution Press, (2010).

²²Hansen. & Nissenbaum, H., 2009. *Digital Disaster*. Cyber Security and Copenhagen School. *International Studies Quarterly*, Volume 4

1.7 Hypotheses

- a. Counter cybercrime challenges in Kenya have been adequately addressed
- b. Counter cybercrime policies and strategies in Kenya have been fully implemented

1.8 Research Methodology

Research methodology explains the study's systematic processes, which include accounting for the study's design, selection procedures, data collection tools, and data analysis techniques. A comprehensive examination of the issues confronting African counter-cybercrime in the twenty-first century: A qualitative research strategy that includes desk study of books, review of journal articles, and academic papers on cybercrime was employed to conduct a focused comparison of Kenya and Rwanda. The earlier strategy was supplemented with an analytical and descriptive research method. This article looked at the issues of combating cybercrime around the world, in particular in Rwanda and Kenya. The two methodologies provided a clear picture of the current status and challenges in addressing cybercrime internationally, regionally, and specifically in Rwanda and Kenya. The approach used produced a summary of the study design that was appropriate and supplied a good knowledge of the issues in the subject area. This study aims to demonstrate the necessity to address the issues in combating cybercrime by including both quantitative and qualitative data.

1.8.1 Study Design

The study used a variety of methods, including exploratory, descriptive, and comparative research, to discover and compare Kenya's and Rwanda's ways to combating cybercrime

concerns. Before beginning data collection, this study took into account a number of aspects. First and foremost, the people who would be studied were chosen based on their understanding of cybercrime. Other characteristics were the unit of analysis, the scope of the study, the selection of cases, and the data gathering procedures. In Kenya and Rwanda, the respondents were key informants who were strictly people with knowledge of cybercrime or cyber security.

1.8.2 Sampling Procedure

Experts in counter-cybercrime, information, communication, and technology from both the corporate and public sectors made up the target population. A total of 150 people who interact with the subject on a daily basis were interviewed. As a result, the respondents included Defense Forces, National Police Services, Directorate of Criminal Investigations, National Counter Terrorism Centres, Information and Communications Technology Authority (ICTA), and Ministries of Foreign Affairs, all of whom are key stakeholders in the fight against cybercrime.

1.8.3 Methods of Data Collection

Closed and open-ended surveys and questionnaires, key informant interviews, and secondary data will be employed as data gathering instruments. The confidentiality of any information provided will be adequately communicated to participants/respondents. The methods listed below will be used.

i. Survey

Both qualitative and quantitative methodologies were used in this study. Mixed research was beneficial since it improved the outcomes of discoveries and the quality of the educational research.

ii. Key informants

The key informants were interviewed using a standardized questionnaire distributed to important stakeholders in the field of cyber security and counter-cybercrime. Key informant interviews were used to gather a wide range of firsthand information from respondents, including professionals, practitioners, and anybody else with practical experience of cybercrime. They were all chosen for their extensive expertise and grasp of the subject. This research will focus on a representative sample of four key informants chosen at random from each of the following ministries and departments, for a total of forty key informants. Kenya Defense Forces, Police Headquarters IC3, Cybercrime DCI Headquarters, Anti-Terrorism Police Unit, Director of Public Prosecution, Attorney General's Office, Ministry of Interior, private cyber security practitioners, and the International Police Office.

iii. Secondary data

Secondary data will be gathered from other researchers' works, reports from trustworthy sources, and official publications.

1.8.4 Analysis of Data

The data was sorted and analysed utilizing the most up-to-date document analysis and theme methodologies depending on the field of study's emerging difficulties. The respondents' personal information was only utilized for the purpose of this study, and they were not asked to divulge any other source of their responses. For clarity, the data were displayed in the form of narratives, frequency tables, and bar graphs.

1.9 Scope and Limitation

This research focused on the challenges facing counter-cybercrime in the 21st century Africa, a focused comparison of Kenya and Rwanda. The study narrowed down to examine various challenges facing different countries in countering cybercrime, and methods successfully used to counter cybercrime challenges at the international and regional levels, with specific reference to Rwanda. The focus population comprised of key stakeholders in Kenya's ministry of information and technology, security officers deployed to counter cybercrime and private practitioners in ICT. For Rwanda the study focused on both primary and secondary sources to identify methods successfully used in countering cybercrime.

The first limitation was funding because this study was not sponsored by any organization, department or individual. This limitation was addressed using the available resources to achieve this noble goal. Secondly some of the targeted population were not willing to participate in the interviews because they considered information sought to be sensitive and treated as confidential by their respective departments and institutions. This limitation

was taken care of by explaining to the respondents in clear terms and reassuring them that the research was strictly for scholarly purpose and nothing else. The last challenge for this particular study was the fact that there have been few similar studies in the subject in Africa and especially in Kenya and Rwanda, thus resulting to scarce literature to rely on. This limitation was surmounted by reviewing literature about studies done in the field but covering different geographical regions internationally without losing focus of the primary objectives of the study in question.

1.10 Chapter Outline

This study is organized in five chapters as follows: -

- Chapter 1 – This is the introductory chapter covering the introduction, statement of the problem, literature review, objectives of the study, justification of the study, theoretical framework, research hypotheses methodology, scope and limitation of the study.
- Chapter 2 – This chapter looks at the challenges facing counter-cybercrime at a global level.
- Chapter 3 – This chapter evaluates the challenges of counter cybercrime in Africa
- Chapter 4 – This chapter makes a critical comparison between the challenges affecting counter-cybercrime processes in Kenya and Rwanda. This chapter also addresses data collection and analysis to draw findings from the study.
- Chapter 5 – The chapter makes a summary of the study, draws conclusions from the study and make recommendations.

CHAPTER TWO

CHALLENGES FACING COUNTER-CYBERCRIME AT GLOBAL LEVEL: AN ASSESSMENT

2.1 Challenges Facing Counter-Cybercrime at Global Level: An Assessment

For a long time, international efforts to combat cybercrime have been made through the use of laws and regulations, but the plague has persisted rather than decreased. The frequency and sophistication of cybercrime challenges has been noted with great concern; this development has been attributed to the current circumstances, in which, despite efforts to curb the wave of counter-cybercrime challenges, criminals are busy inventing methods and means to frustrate international efforts to address the problem.²³ In this chapter, some of the counter-cybercrime concerns that have allowed cybercrime to persist are examined.

2.2 Inadequate Legislation

Despite the existence of global judicial tools, the disparities between national legal frameworks and international machinery in most circumstances prove to be a severe stumbling barrier to international criminal investigations and prosecutions of computer crimes. This is due to the reversal of international instruments into local legislation on a partial basis. The key distinction is in the prohibition of certain behaviours and procedures for investigating cybercrime and gathering electronic evidence.

Many researches on how to develop coordinated computer crime and cybercrime legislation in many parts of the world have been on-going for some time, according to

²³ Ajayi, E F G, Journal of Internet and Information Systems, Challenges to Enforcement of Cyber-crimes Laws and Policy, School of Law , Kenyatta University Nairobi Kenya

Alkaabi Ali. That is, a legislation addressing cybercrime is constantly being established, including in industrialized countries.²⁴ Even though most countries in the world are linked to the Internet, many of them have not yet put in place criminal laws and regulations to regulate cybercrimes, and for the few that have, the encounters and inconsistencies in the laws make it problematic or incredible to examine, put on trial, and even castigate cybercriminal conduct, according to a 2009 report by the International Telecommunication Union (ITU). The scenario has remained unchanged for the past twelve years, adding to the many obstacles of combating cybercrime.

All nations must pay immediate attention to the lack of a worldwide harmonized legal framework for cyber-criminal activity, which has become a problem."²⁵ Even while numerous nations have taken the lead in enacting legislation to prevent computer-related crimes, many more countries have yet to enact legislation to prohibit the misuse and exploitation of computers. As a result, the difficulty in combating cybercrime has been mostly attributable to limited regulation and the ineptness of those that do exist. It is critical to remember that, while there are laws against cybercrime, the provisions of those laws and regulations are insufficient to deter cybercriminals from their illicit actions. In Australia, for example, there are various laws that make cybercrime illegal. This includes, but is not limited to, the Computer and Telecommunications Services Offenses Act 1979, the Telecommunications (Interception and Access) Act 1979, the Criminal Code Act 1995,

²⁴Ali O. S, Alkaabi Combating Computer Crime: An International Perspective, Thesis submitted in accordance with the regulations for the Degree of Doctor of Philosophy, Queensland University of Technology, 2010

²⁵International Telecommunication Union. ITU Toolkit for Cybercrime Legislation. 2009 Updated in February 2010, available from: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf>.

and the Cybercrime Act of 2001. Except for child phonograph, all of the above mentioned laws and regulations prescribed punishments of one to three years in prison. It is clear that the nature of the law is insufficiently punitive to deter cyber criminals from carrying out their illegal activities; even if existing laws were strictly enforced, the impact would be minimal or non-existent because the sentence could not possibly be deterrent. This contributes significantly to the global challenges of combating cybercrime.

2.3 Law Enforcement Challenges

Cybercrime is becoming more common, and it now has an international dimension.²⁶ One of the reasons for this is that the criminal does not need to be physically present at the location where the service is provided in order to commit a crime.²⁷ Another stumbling block is the lack of a complete international legal framework and a supranational entity capable of investigating cybercrime and other transnational crimes, which necessitate collaboration among various authorities in all nations concerned.²⁸ One of the key obstacles of a globalization of computer-related crimes is the disparity in national laws, restricted instruments, and lack of universal coordination.²⁹ As a result, combating cybercrime has become a major concern.

There are those who argue that international law is not law because it lacks enforcement mechanisms; these proponents argue that there are no specialized trained officers to

²⁶Keyser, The Council of Europe Convention on Cybercrime, *Journal of Transnational Law & Policy*, Vol. 12, Nr. 2, page 289,

²⁷ *Ibidem*

²⁸ Sussmann, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, *Duke Journal of Comparative & International Law*, 1999, Vol. 9, page 451

²⁹ Gabuardi, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, *Mexican Law Review*, Vol. I, No. 2, page 156,

enforce international laws; they believe that international law is not law in practice and that no amount of evidence can persuade them otherwise. Existing laws and policies are divided into quasi-international, regional, and national categories, making them ineffective in dealing with the difficulties posed by cybercrime, which has global jurisdiction. The only law that can directly address the threat of cybercrime is a global law that applies across all jurisdictions. This can only be accomplished if political will is mobilized to enact that universal law; otherwise, mankind will continue to be overwhelmed by the challenges of combating cybercrime due to insufficient mechanisms for enforcing cybercrime laws and regulations. As a result, practical counter-cybercrime laws and regulations will continue to face enforcement difficulties. This is a worldwide problem, and unless it is handled on a global scale, cybercriminals will always get away with it.

2.4 The Question of Jurisdiction

Another issue that undermines efforts to combat cybercrime is the issue of jurisdiction. At the global level establishing adequate controls to standardize the collecting, and safekeeping of evidence from Electronic Service Providers, which are usually located in many countries, is difficult and time-consuming.³⁰ When sovereignty and territorial integrity are taken into account, each sovereign nation across the world stamps its power and makes laws binding to everyone and everything within its geographical entity, which is why different sovereign states make regulations on the same matter in varied ways, resulting in conflicting laws. The issue of jurisdiction is frequently at the heart of any

³⁰Common challenges in combating cybercrime As identified by Euro just and Europol June 2019, Joint Report, Europol and Euro just Public Information

decision made by a court with competent authority. When a court law has no jurisdiction, it also means that it lacks the required capability to adjudicate any case under that jurisdiction. Even if the case is watertight, a lack of competence is devastating since it renders proceedings worthless and void. The issue of jurisdiction in the execution of cybercrime legislation centres on geographical jurisdiction and judicial jurisdiction.³¹ Cybercrime is separate in nature; it belongs to a peculiar category, is exclusive and discrete in character, and differs from conventional crimes committed in the same geographical location as the culprit and the victims. Victims in the same geographic place are likewise directly affected. Unlike traditional crimes, cybercrime crosses regional and national borders; this is known as cross-border or international crime. As a result, cybercriminals can operate peacefully from their homes, businesses, cafes, or anyplace else they want, as long as they have a computer desktop, laptop, tablet, or even a phone linked to the Internet. This demonstrates that information in modern technology communication systems renders the geographical location of perpetrators and victims of crimes irrelevant. Physical contact between the criminal and the victim of a crime is not required.

2.5 Counter Cybercrime Challenge of Extradition

The extradition of a criminal suspected to have committed a crime in another state is described by the Oxford Dictionary of Law as; the surrender of a person accused of committing an offence in the requesting state by the host state.³² It refers to the procedure of transporting a suspect, a criminal, or an accused individual to a separate legal authority

³¹ Ajayi, E F G, Journal of Internet and Information Systems, Challenges to Enforcement of Cyber-crimes Laws and Policy, School of Law , Kenyatta University Nairobi Kenya

³²Oxford Dictionary of Law, 2002

for trial or punishment where the claimed offense occurred. Although due to the idea of state sovereignty, things are different in practice. Under international law, there is no process that requires sovereign governments to immediately surrender cybercriminals for trial as a matter of course. As a result, most nations where cybercriminals are identified refuse to extradite them to the requesting countries; complicating the implementation of cybercrime laws and regulations around the world.

Another principle that must be met in the extradition procedure is dual criminality. In order for a suspect to be extradited to the requesting state, the claimed offense must be punishable within the jurisdiction of the state to which extradition is sought. Inhumane treatment, such as degrading punishment and torture, which is likely to be meted out to the suspect, is a bar to extradition. In addition to the aforementioned, a request for extradition of a suspect may be declined if the alleged offence is classified or considered as political. The exceptions in extraditions based on political motives are those broadly classified as purely political offenses directed against governments, for example treachery, subversion, spying, and other relatively sensitive political offenses dedicated for political reasons, in a radical context, or in connection with a dogmatic act.

2.6 Ineffective Reporting and Shortage of Cybercrime Data

Several countries throughout the world have come up with adequate laws and policies to combat cybercrime, but the challenge is enforcing those laws and policies, as well as the absence of proper reporting of cybercrime events to appropriate international agencies. As a result, this trend has become a stumbling barrier for international attention and

understanding of the magnitude of cybercrime risk.³³ The lack of collaboration between the police and other agencies responsible with the inquiry and trial of cybercriminals on one hand, and the victims, other stakeholders, and witnesses on the other, is closely tied to the unwillingness to disclose cybercriminals. It makes no difference whether the victims are private, corporate, or institutional institutions. According to the United States of America government, the annual data collected on cybercrime events is way below the actual figures.³⁴ The FBI's IC3 program publishes annual reports that include the number of cybercrime events in the United States.³⁵ However, this figure only includes incidents that are reported directly by victims via the IC3's internet platform.

However, the IC3 estimates that this number represents only 10-12 per cent of all incidents that occur in the country, because most victims do not report their repression.³⁶ According to non-government sources, the problem is far more serious than it appears. Reporting cyber-attacks is seen as exposing the weaknesses and vulnerabilities of their systems in relation to competing businesses. This conduct deflates the client's self-esteem and may result in customer dissatisfaction. Most business proprietors and operatives would rather remain silent and try to patch their systems as much as possible than report to the authorities in charge of combating cybercrime in this situation. One of their sons has been given for refusing to report cybercrime because of the costs associated with following up on the cases, which in most cases outweigh the benefit derived.

³³ Ibidem

³⁴Ishan Mehta, The Need for Better Metrics on Cybercrime, Third Way (2019) Stable URL: <https://www.jstor.org/stable/resrep20149> Accessed: 14-03-2020 07:47 UTC

³⁵Filing Complaint with the Internet Crime Complaint Centre (IC3), Federal Bureau of Investigation, and www.ic3.gov/.

³⁶Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." The New York Times, the New York Times, 5 Feb.

2.7 Identity of Cybercriminals

One of the most significant impediments to global attempts to slow down the spread of cybercrime is the difficulty of identifying cybercriminals. It's tough to classify people's actions in terms of who's doing what and where they're on the Internet at any particular time. Because the global information system is open to everybody, any user can log in and communicate with anyone, anywhere in the world, with no constraints because there are no requirements to meet. As a result, hackers can mask their identity using various telecommunications equipment and create difficult in tracing their identity using online Internet Protocol (IP) address of any user, thanks to the freedom of information and communication.³⁷

Tools such as Psiphon and the Onion Router (Tor), frequently conceal Internet users' identities and communication is frequently routed through multiple servers, making it even more difficult for cybercriminals to be tracked.³⁸ No matter how well-crafted or intended laws can work as long as the names of cybercriminals remain unknown because the law does not work in a vacuum. Any law(s) put in place becomes null and void if the criminals are not identified. To put it in another way, cybercrime laws were designed primarily to apprehend and prosecute cybercriminals as and when they committed crimes.

³⁷Ajayi, E F G, Journal of Internet and Information Systems, Challenges to Enforcement of Cyber-crimes Laws and Policy, School of Law , Kenyatta University Nairobi Kenya

³⁸Ibid

2.8 Nature of Evidence

Another hurdle to combating cybercrime is the sort of evidence available. The growing use of ICTs and digitalization has had a significant impact on the methods for gathering evidence and using it in court.³⁹ Since digital evidence presents particular obstacles, it necessitates specific processes.⁴⁰ Maintaining the integrity of digital evidence from the time it is obtained until it is presented in court is one of the most difficult parts. The danger with digital data is that it is extremely fragile and can be erased or changed at any time. This is especially true for data stored in random access memory, which is eventually erased when the machine is shut down, necessitating greater data preservation skills.⁴¹

The law of evidence encompasses all of the laid down procedures that apply to the systematic presentation of facts and proof in court proceedings. In contrast to evidence given in traditional crimes, where physical evidence could be offered to the court in order to secure the accused's conviction, physical evidence in cybercrime prosecution is not common. Cybercriminals have also been known to wilfully destroy evidence in order to avoid being prosecuted and convicted.⁴²

³⁹Casey, Digital Evidence and Computer Crime, 2004, page 11; Lange/Nimsger, Electronic Evidence and Discovery, 2004, 1; Hosmer, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1,

⁴⁰Moore, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004,

⁴¹Casey, Digital Evidence and Computer Crime, 2004

⁴²Moore, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004,

2.9 The Cost and Time Factor in Investigations and Prosecution

The cost of the investigations and forensic evidence required in the prosecution of cybercrimes as a scientific crime solving approach is in itself expensive as opposed to gathering physical evidence in traditional crimes.⁴³ This is because of the advanced equipment, materials, and expertise required in conducting such investigations. Many complications arise when a criminal is sought extraterritorially, resulting in increased costs in the investigation of cybercrime in terms of travelling and accommodation. These include, but are not limited to, air flights where investigators must be physically present in a different jurisdiction.

2.10 Issue of Training and Poor Remuneration for Law Enforcement Agencies

'Rubbish in, rubbish out' is a proverb that refers to the dangers of entrusting a serious activity to people who aren't well-trained or capable of securing evidence of cybercrime.⁴⁴ Unless officers are well equipped and competent even with robust functional and procedural domestic criminal legislations and acquiescence to international instruments such as the Budapest Convention, investigations may yield little results. The broader criminal justice system faces a tremendous challenge in communicating a shared understanding of the essential technical skills, information, and duties done throughout investigations and prosecutions.⁴⁵

⁴³Ajayi, E F G, Journal of Internet and Information Systems, Challenges to Enforcement of Cyber-crimes Laws and Policy, School of Law , Kenyatta University Nairobi Kenya

⁴⁴Cameron S. D. Brown, International Journal of Cyber Criminology Vol. 9 Issue 1 January – June 2015 Australian National University, Australia

⁴⁵Graycar, A. (2001, June 21-22). New crimes or new responses. Speech presented at 4th National Outlook Symposium on Crime in Australia: New Crimes or New Responses. Canberra: Rydges Lakeside.

2.11 Loss of Cybercrime Data

The European Court of Justice nullified the Data Retention Directive on April 8, 2014, leaving law enforcement and prosecutors uncertain about their ability to seek data from private parties. As a result of the Court of Justice of the European Union's decision, national legislation in various European Member States has been overturned. Although Internet Service Providers in some Member States retain some data for commercial or accounting purposes, they do not have any data available to support criminal investigations. Such inconsistencies obstruct the work of cyber-competent authorities, resulting in the loss of investigative leads and, eventually, the capacity to prosecute criminal activities online efficiently. The lack of a consistent retention of electronic communication data across the European Union has been a major difficulty in investigating cross-border cybercrime since the court's rulings. Both agencies' combined experience has shown that electronic communication data is critical to the successful investigation and prosecution of serious crimes, including cybercrime. Law enforcement efforts to investigate and attribute crime have been hampered by a major online capability gap caused by carrier grade network address translation (CGN) technologies. The threat of data loss is exacerbated by ISPs' widespread use of (CGN) technologies.

2.12 The Challenge of New and Emerging Technologies

Organizations are perplexed by how to acquire new platforms and intelligence to do so as well as by how to defend their structures, thanks to today's complex and disruptive technologies, as well as new cyber tools and threats that emerge every day.

(i) Challenge of web servers' protection

One of the challenges persistently associated with countering cybercrime is attacks on the web applications to extract data or distribute malicious code. Malicious code is distributed by cyber criminals via their legitimate web servers they have managed to compromise making it difficult to counter cybercrime. The importance of protecting web servers and web applications must be prioritized. It is strongly recommended that you utilize protected, safer browsers when conducting significant transactions.

(ii) Challenge of Cloud Computing and its services

In the recent past, adopting cloud services was slowly welcomed by all small, medium and large scale enterprises. As a result, the entire globe is gradually moving towards embracing the clouds technology. This tendency postures a substantial challenge for cyber security because movement of information and data can bypass traditional checkpoints. Policy controls for web applications and cloud services must develop as the number of applications available in the cloud grows in order to prevent the loss of vital information. Although the cloud offers numerous advantages, it is important to remember that as the cloud evolves, so do its insecurity issues evolve.

CHAPTER THREE

CHALLENGES OF COUNTER-CYBERCRIME EFFORTS IN AFRICA

3.1 Challenges of Counter-Cybercrime Efforts in Africa

Before the emergence of Information Communications Technology, Africa was seen as a "dark continent" (ICT). As a result, it was expected that the development of ICTs would lead the way and connect the region to the rest of the globe, so integrating it into the global community.⁴⁶ Africa has been exposed to the unintended repercussions of cybercrime as a result of this new trend. Most governments were caught off guard by the manifestations of cybercrime, their far-reaching ramifications, and the potential for devastating harm rather than good. Laws in existence, regulations, and organisations were incapable of keeping up with the region's distressing rate of cybercrime permeation.⁴⁷ Most governments have taken concerted steps to address this problem, albeit their efforts to combat cybercrime have been generally ineffectual.

The increase in broadband admittance has resulted in an increase in internet users, making it possible for cybercrime to thrive on the African continent. Most African nation states are faced with more demanding concerns such as poverty, the HIV/AIDS pandemic, the fuel predicament, political and ethnic unrest, traditional crimes, and the Covid 19 pandemic. As a result, they are falling behind in the war against cybercrime because it is not given the precedence it deserves. The problem has been exacerbated by the public's lack of understanding of information technology and the lack of appropriate legal

⁴⁶Eric Agwe, etal, *Combating Cybercrime in Sub Sahara Africa; A Discourse on Law, Policy and Practice*, Nelson Mandela School of Public Policy, Southern University Baton Rouge, Criminal Justice Department, Southern University Rouge, January 2011.

⁴⁷ Ibid

frameworks to deal with cybercrime at the regional and national levels. Some African governments have put in place measures to help combat the threat of cybercrime, but they have so far failed.

3.2 Challenge of Jurisdiction

The legal power of a court to hear and decide judicial actions concerning a certain matter is referred to as jurisdiction. It also refers to the court's ability to rule on issues pertaining to the topic of the dispute. Only when a court of law has jurisdiction over the place where the crime is committed can it exercise judicial powers. Jurisdiction is a threshold issue that is critical to the hearing of a case, and it frequently extends beyond the Court of Law's ability to adjudicate and determine judicial processes. It is the authority to decide on problems pertaining to the controversy's subject matter.⁴⁸

With the introduction of contemporary knowledge, new categories of crime have developed, while conventional crimes such as fraud are perpetrated using sophisticated skills. The cybernetic borderless world has provided a platform for crime, disassembling old barriers.⁴⁹

Scholars, governments, and other interested parties have paid close attention to the global aspect of cybercrime. Cybercrime is one of the most renowned cross-border crimes, and it has gotten worse as the usage of computer networks has grown. "With the ever-expanding information infrastructure, countless incidences of international hacking, and

⁴⁸ Brenner and Bert-Jaap Koops, 'Approaches to cybercrime jurisdiction' (2004) *Journal of High Technology Law*

⁴⁹S.Maat, *Cybercrime: A Comparative Law Analysis*, Unpublished, LLM dissertation, University of South Africa (2009)3.

the increasing likelihood of expanded global espionage, it is critical that governments have jurisdiction over international computer crime matters."⁵⁰ "The virtual world appears to be a borderless environment," according to Goodman and S Brenner, "and this makes Cybercrime easy to perpetrate, requiring just a few resources, and it can be committed in a given jurisdiction without the offenders being physically there."⁵¹

Cybercrime bypasses the issue of jurisdiction and does not necessitate physical proximity between the victim and the perpetrator, adding to the difficulty of detection. Furthermore, additional resources are needed to follow down cyber offenders in many nations, and deficient criminal laws governing cyberspace sometimes result in few successful convictions due to jurisdictional issues.⁵² For the reason that cyber-crime is worldwide in nature domestic measures are rendered ineffective. Individuals or criminals are frequently unknown at first, and the space and dimension of interference may be unknown. Jurisdictional difficulties are complicated by the ability to access and destroy computer systems from anywhere on the planet. Most Internet service providers are dependent on services provided outside Africa. Internet service providers may rent out web space in one country based on the availability of specific hardware in another.

In order to successfully investigate cybercrime offences, law enforcement authorities from all countries involved must cooperate and work together, especially when the perpetrators

⁵⁰ Cybercrime and Intellectual Property section of the National Information Infrastructure Protection Act of 1996: Legislative analysis (U.S. Department of Justice)

⁵¹ Goodman & S Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' 2002 International Journal of Law and Information Technology 139-223 at 142, 146-150.

⁵² Renner 'Cybercrime investigation and prosecution: the role of penal and procedural law' 2001 Murdoch University Electronic Journal of Law

and targets are situated in separate countries. However, due to the countries' national independence, no investigations are permitted within their borders unless local authorities have given their approval.

All countries engaging in cybercrime investigations require the cooperation and participation of the ruling classes. Because standard mutual legal assistance concepts do not function in cybercrime investigations, cooperation cannot be founded on them. Investigations are frequently delayed due to the time required to coordinate with foreign law enforcement authorities and formal procedural processes. Vital data for tracing perpetrators is frequently obliterated by criminals after a short while. Understanding cybercrime phenomena, problems, and legal responses to the traditional mutual legal assistance system can take a long time to put together, making the short investigation period problematic.

When perpetrating the crime, cyber criminals do not need to be present at the same location as the target. Many cybercrime offenses are transnational in nature since the criminal's location may be completely different from the act. International cybercrime offences require a significant amount of effort and time, as they look for ways to evade countries with strict cybercrime legislation.

Preventing "safe havens" is one of the most difficult issues in the fight against cybercrime. As long as "safe havens" are in existence, perpetrators will utilize the same to thwart inquiries. To evade detection and prosecution, criminals may seek to base themselves in

nations that have not completely enacted cybercrime legislation, making those countries vulnerable. Due to limited regulation, particularly in countries where criminals choose to reside, it may be difficult to manage significant cybercrime offenses affecting victims all over the world. As a result, certain governments may face increased pressure to implement legislation and address the problem. For example, in 2006, a Philippines suspect created the "Love Bug" worm, which infected many computers in the world.

Local investigations were hampered by the fact that the development and propagation of dangerous software worms was not effectively criminalized in the Philippines.

3.3 Challenges of Cybercrime Legislation

"The electronic media challenges the laws intended or made to operate in a physical medium," says one expert."⁵³ Furthermore, in many circumstances, laws relating to conventional crimes cannot be extended to cover crimes committed by automated methods. "Cybercrime is fast evolving and flourishing all over the world. Cyber criminals utilize sophisticated tactics to steal data and people's identities, scam mobile phone customers, and carry out corporate espionage, among other crimes."⁵⁴

The legitimate structures of African countries were founded on the vestiges of colonial laws. Because the British were their colonial overlords, countries like Nigeria, Kenya, and Uganda had laws based on British common law, while others like Ivory Coast, Gabon, and the Democratic Republic of Congo had laws based on French civil law. Countries like

⁵³M. Watney 'The Evolution of legal regulation of the Internet to address terrorism and other crimes' (2007) 3 *Tydskrif vir die Suid-Afrikaanse Reg* 469

⁵⁴ G. Gordon 'The hidden economy of cyber-crime' *Sunday times* 12 February 2012.

Cameroon, which had both British and French colonial masters, faced a more difficult situation. Dealing with both Civil and Common Laws at the same time proved to be a difficult task. Due to disparities in legal systems, different African countries tackled cybercrime differently, resulting in a lack of coordination. Cooperation in combating cybercrime and prosecuting perpetrators becomes difficult when one country's laws prohibit specific acts while another country's laws do not punish them to the same extent.

The illicit actions have required the creation of international collaboration networks aimed at facilitating proactive cybercrime prevention initiatives and the enactment of effective cybercrime legislation. South Africa was named the sixth most targeted country in the world for spear-phishing by the Federal Bureau of Investigation (FBI). "Hackers have attacked South African government agencies, financial enterprises, banks, and other private industry with malware and other cyber threats."⁵⁵

Preceding the depiction of the Automated Infrastructures and Transactions Act in South Africa, the common law and legislative law were extended as extensively as feasible to allow for the arrest and punishment of some online criminals (ECT). "When it comes to internet offenses, the common law's applicability has its own limitations and narrows dramatically."⁵⁶

⁵⁵ M Sulfab 'Challenges of cybercrime in South Africa', research paper for Master of Arts in national security studies, American Military University (2014) 9.

⁵⁶ Ssnail 'Cybercrime in South Africa-Hacking, Cracking and Other Unlawful Online Acts' (2009) *Journal of information, law and technology*

3.4 Evidential Challenge

The mechanism through which facts relevant to an accused person's guilt or innocence are established at a hearing is evidence. It is usual to lose or contaminate evidence during investigations, as well as other obvious issues that may impair the portion of evidence's accuracy, or even threaten the entire criminal proceedings.⁵⁷ One of the most important issues that has also shown to stymie cybercrime investigations and prosecutions is data collection from outside territorial boundaries, while digitization and the evolving use of information technology has a significant impact on evidence gathering and use in court of law processes.⁵⁸ Honorable Courts use the rule of evidence to determine which facts are supported by evidence and are legally binding and admissible, and which ones are not.⁵⁹ The Economic Community of West African States (ECOWAS) issued a directive in which it said that "electronic evidence shall be considered as proof to establish an offence" (Article 32).

The second leg of Article 32's regulations stipulated two additional qualifications for recognizing these pieces of evidence: first, that "the source can be identified," and second, that "they be stored in such conditions as to insure their integrity."⁶⁰ These conditions,

⁵⁷ Erin Murphy, 'The new forensics: Criminal justice, false certainty, and the second generation of scientific evidence' (2007) *California Law Review* 721-797; Cynthia E Jones, 'Evidence destroyed, innocence lost: The preservation of biological evidence under innocence protection statutes' (2005) *Am Crim L Rev* 42,

⁵⁸George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, and Alan Schwartz, 'Information Technology Security Handbook' (Washington, DC: World Bank, 2003)

⁵⁹ Ian Volek, "Federal Rule of Evidence 703: The Back Door and the Confrontation Clause, Ten Years Later" (2011) *Fordham L REV*, 80, 959,

⁶⁰Chibuko Raphael Ibekwe, Thesis submitted to School of Law, University of Stirling The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions, July 2015

however, have not been qualified in any way by the directive and hence cannot be legally obligatory.

Although automating the entire investigative process is tough, complex, and expensive, law enforcement organizations can employ the expanding power of computer systems and specialized forensic software to speed up investigations, gather evidence, and automate search operations. The offender can digitally alter images to avoid detection and make it difficult for investigators to determine the genuine identities of the perpetrators. While a keyword-based search for unlawful content can be done quickly, identifying illegal pictures is more challenging.

To conduct investigations, responsible authorities will need Internet-specific techniques and instruments. "In this case, instruments to identify the culprit and collect the evidence required for criminal procedures are critical."⁶¹ Traditional investigation tools are insufficient to identify an offender in a rising environment of Internet-related cybercrime incidents.⁶² Countries have recently developed investigation tools, such as monitoring, that permit them to capture both cable and cellphone calls. Traditional voice calls are typically intercepted by telecom companies using the VoIP paradigm. "If a service is based on peer-to-peer technology, service providers may be unable to intercept communications because the relevant data is exchanged directly between the communicating

⁶¹Goerling, The Myth of User Education, 2006 at www.parasiteeconomy.com/texts/StefanGorlingVB2006.pdf.

⁶² Swale, Voice Over IP: Systems and Solutions, 2001; Black, Voice Over IP, 2001.

participants."⁶³ This necessitates the development of new technology solutions as well as legislative mechanisms.

The unique concerns that come when addressing digital evidence need the engagement of specific methods. Maintaining the veracity of electronic evidence is one of the most difficult parts. Digital data is enormously delicate and can easily be erased or revised if not properly preserved. This is particularly factual of evidence kept in the system memory of Random-Access Memory (RAM), which is inevitably obliterated when the system is turned off and thus necessitates the use of special preservation techniques to keep it. Investigators were able to focus on the suspects' properties in the recent past when searching for computer detention. Investigators must now focus on the likelihood that digital information is held out of the country and may only be repossessed remotely if necessary.

The methods, by which digital evidence is acquired, as well as the processes concerning the presenting of the same digital evidence in court, deserve special consideration.

3.5 Challenges of Extradition

The prescribed process of requesting the surrender of an offender from one territory to another for the purposes of prosecuting the offender, sentencing the offender for an offense for which the person has already been convicted, or carrying out a sentence that has already been passed against the offender is referred to as extradition.⁶⁴ Extradition is

⁶³Bellovin et al, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP; Simon/Slay, Voice over IP: Forensic Computing Implications, 2006;

⁶⁴Zsuzsanna Deen-Racsmany, 'Active personality and non-extradition of nationals in international criminal law at the dawn of the twenty-first century: adapting key functions of nationality to the

usually the result of an agreement between two states, and it is more of a matter of international commitment than a legal need. It is underpinned by bilateral treaties between the parties, which are codified in each state's domestic legislation.⁶⁵ Unless it has signed a bilateral or multilateral agreement with the asking countries, no government is obligated to release a person who is on its territory.

3.6 Challenges of Dual Criminality

For the dual-criminality principle to apply, a person may be extradited only if his or her actions are criminal in both the requesting and requested nation states.

To be extraditable, an offense must be punishable under both the surrendering and requesting countries' criminal laws. Some African countries have criminalized cybercrime and established regulations, whereas others have not enacted cybercrime legislation and hence cannot extradite suspects.

When an offense is outlawed in one of the states affianced in the investigations but not in the other, the idea of dual criminality is put to the test. By including third countries in their attacks, criminals may make investigations more problematic. Cyber thieves operating out of nations with lax cybercrime laws may choose targets from any country, including those with severe rules, and vice versa.

requirements of International Criminal Justice' (2007) Doctoral dissertation, EM Meijers Institute of Legal Studies, Faculty of Law, Leiden University

⁶⁵ Satya Deva Bedi, 'Extradition in international law and practice' (Rotterdam, 1966) 69; Bassiouni M. Cherif, "Political Offense Exception Revisited: Extradition between the US and the UK-A Choice between Friendly Cooperation among Allies and Sound Law and Policy" (1986) *The Denv J/Int'l L & Ploy*, 15, 255.

3.7 Challenges of legal and International Cooperation

Cybercrime is by its very nature international, spanning both territorial and geographical barriers. "Because they are unrestricted, successful investigation and prosecution needs international cooperation between states." Article 23 of the Council of Europe's Convention on Cybercrime lays out the bases for intercontinental cooperation in cybercrime investigations and prosecutions. "Because it is designed to be a regional unifying convention for member states, the African Union should have set precise provisions for terms and means of cooperation, and if possible, stipulate punishments in case of failure or neglect by member states to cooperate."⁶⁶

Serious cooperation exists only in the form of word of mouth, not in the form of acts. In the fight against cybercrime, the African Union has done very little to bring countries together. The problem of cybercrime has never been treated seriously as a continental issue. The Australian government has not taken cybercrime seriously enough. The African Union has not organized itself to create an AU police force or agency that is appropriately prepared to deal with cybercrime issues, similar to how there is an AU peacekeeping force that deals with violence in Africa. Such a force or service would be dispatched to nations where cybercrime is prevalent.

Declaring cybercrime, a war in the region will save it from unhappiness and prevent it from being at the pity of regional blocs and individual countries that lack the synergy and

⁶⁶ Lilly Pijnenburg Muller, 'Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities' (2015)

will to combat cybercrime. Uniform regulations to combat cybercrime and deal with the problem of suspicion and mistrust between countries would be extremely beneficial.

3.8 Challenges of Anonymity of Criminals

The anonymity that information and communication technology provides consumers makes combating crimes difficult. Individuals can engage in criminal activities without revealing their true identities or actions to others, makes it difficult for law enforcement to track down the committers and bring them to justice.

Similarly, using anonymous proxy servers hides the user's identity data by masking the Internet Protocol address and replacing it with another IP address. The dispersed nature of the network and the accessibility of some Internet services cause confusion of origin although verifying the origin of communication is a vital component of cybercrime investigations, this makes it difficult to identify cybercrime perpetrators. Unidentified communication could be the outcome of providing a service or performed with the intention of remaining anonymous to the victim's detriment. Though being aware of the source's ambiguity is critical in avoiding erroneous judgments.⁶⁷

Criminals may utilize Subscriber Identification Module (SIM) cards and vulnerable private wireless networks from nations that do not require comprehensive personal information after registration to carry out illegal activities. It is not clear now if the

⁶⁷Casey, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2.

limitation of anonymous communications and unidentified Internet entree should play a larger role in the battle against cybercrime.

3.9 Challenge of Reliance on Information and Communication Technologies

Almost every area of daily life, including Information and Communication Technologies (ICTS), is subject to regulatory and oversight activities. Over-reliance on ICT has resulted in Attacks on systems and services are increasingly likely.

Monoculture and homogeneity of operating systems are flaws in the current technical architecture. Many private users of Small Medium Enterprises utilize the Microsoft Operating System, making it simple for thieves to develop offensive attacks by focusing on recognized susceptible targets. The advent of has enabled developing countries, including African countries, to build cheaper infrastructural technologies like Wimax, allowing them to provide internet services to a broader population, exposing more individuals to cybercrime and increasing the number of targets or victims.

Most African governments are concentrating their efforts on increasing internet connectivity while underinvesting in cybercrime prevention. As a result, there are insufficient safety measures in place, as security measures necessitate a significant upfront expenditure that most African countries cannot afford.

3.10 Challenge of Readily Available Devices and Ease Access

To commit cybercrime, a criminal requires only the most basic of tools. Committing cybercrime necessitates technical know-how, hardware, and software, as well as internet connection. Serious cybercrime can be committed with readily available devices that are quite inexpensive. Cybercrime has been made easier, though, thanks to specific software tools. With enough expertise, cyber hackers can obtain software programs designed to detect havens or defeat secret code security. Due to cloning techniques and give-and-take trade, limiting the general availability of such gadgets on the market is challenging.

The most common method of connecting to networks is "wardriving," which is the phrase used to describe the process of looking for available wireless networks.⁶⁸ This allows thieves to gain access to networks with relative ease and anonymity. There have been obstacles in the fight to restrict unrestricted access to internet services in order to prevent illegal misuse of these services, as well as to prevent and facilitate investigations, for fear of interfering with the development of E-commerce and the information society as a whole. It is contended that such restrictions would constitute a violation of human rights. This makes it harder for investigators to obtain the evidence necessary for prosecution.

3.11 Challenge of Availability of Information

Every day, the internet contains millions of updated information web pages, which anyone can peruse and obtain at the push of a mouse. The updated data can be used for both illegal and legitimate purposes. For example, a criminal planning an attack might look for

⁶⁸ Ryan, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004,

vulnerable password protection systems or detailed instructions on how to manufacture an explosive device from readily available low-cost materials on the market. In addition, Google for a map of the region he intends to target. Offenders can also use exploration engines to enquire their objects. Using such engines, wrongdoers can get overtly available information that assists in the preparation and execution of their heinous crimes.

3.12 Challenge of Missing Mechanism of Control of the Internet

The internet was created by the military as a military network. This was the foundation for requiring distributed network design to reserve the fundamental functionality essential to power. The network topology of the internet is resistant to nonmilitary enhancement, external control, or change. Initially, the internet was not built to deter external aggression, but rather to prevent internal network attacks and to aid criminal investigations.

With the passage of time, the internet is increasingly being used for civil services. With the transition from military to civil service, the nature of demand for control mechanisms altered. The core control devices do not exist, and retrofitting them would be difficult without significant network reorganization. Cybercrime investigations are extremely challenging, especially in terms of compiling evidence, due to the lack of control devices since the network is based on protocols designed for military reasons.

3.13 Challenge of Encryption Technology

With time the internet is progressively being used for public services. The kind of request for control mechanisms transformed from the military and transitioned to civil service.

The essential control devices do not exist, and retrofitting them without considerable network restructuring would be challenging. Due to the lack of control devices, cybercrime investigations are particularly difficult, especially in terms of assembling evidence, because the network is built on protocols designed for soldierly purposes.⁶⁹ Encryption is the process of converting plain text into a secret design through the use of an algorithm. It remained shrouded in secrecy for a long time, despite the fact that maintaining such concealment in such a tangled setting is difficult.⁷⁰

Because to the integration of encryption know-how in operating systems and the extensive accessibility of easy-to-use software tools, it is now probable to encode computer data with the click of a mouse, increasing the likelihood of law implementation authorities being confronted with corrupted data. Different technical solutions can be used to protect encrypted data, and numerous software tools are available to automate the procedures. Searching for encryption passwords and trying common passwords, researching flaws in the software tools used to file, and long brute-force attacks are some of the encryption tactics employed. "A "brute-force attack" is a method of identifying a code by evaluating every conceivable combination.⁷¹ The encryption can take up to two weeks to break, but if perpetrators employ a 40-bit encryption, it can be broken in under a second utilizing today's computer processing techniques.⁷²

⁶⁹ 2006 E-Crime Watch Survey, page 1, available at: www.cert.org/archive/pdf/ecrimesurvey06.pdf.

⁷⁰ Kahn, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58,

⁷¹ Lowman, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: <http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.Pdf>.

⁷² Jackson/Grunsch/Claypoole/Lamont, Blind Steganography Detection Using a Computational Immune: A Work in Progress, International Journal of Digital Evidence, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf;

3.14 Drafting National Criminal Laws Challenge

Sound legislation is the cornerstone for investigating and prosecuting cybercrime offenses. Given the rapid pace of network technological advancements, legislators must constantly review Internet expansions and the efficiency of existing rules.

The greatest difficulty for the national criminal legal system is the time it takes for possible exploitation of new technologies to be accepted and necessary adjustments to the national criminal code to be made.

Given the rate at which network innovation is accelerating, this dilemma remains as relevant and timely as ever. Many African countries want to catch up with legislative changes and are working hard to do so. The three most significant steps in this process are adjusting the national law, identifying gaps in the penal code, and writing new regulations. Effective legislative foundations can be secured by recognizing the necessity for new technology-specific divisions within national law-enforcement organizations capable of investigating potential cybercrimes and identifying gaps in the penal code. It is vital to compare the condition of criminal legal provisions in national law with requirements deriving from new types of cybercrime offenses. In many circumstances, existing criminal laws can be easily applied to electronic documents if the existing rules are capable of covering new types of offenses. To those offenses that are omitted or poorly covered by national laws, legislative changes can be made. Apart from making adjustments for well-known frauds, lawmakers must constantly examine new and evolving types of cybercrime to ensure their effective prosecution.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.1 Challenges Affecting Counter-Cybercrime Processes in Kenya and Rwanda: A Critical Comparison

This chapter looks at how Kenya and Rwanda deal with counter-cybercrime issues in their respective countries. And to what extent they have succeeded in achieving the much-needed national security. The chapter begins by looking at secondary data on cybercrime before moving on to primary data on the same topic. The available data was analyzed in light of the goals.

The challenge of combating cybercrime is a worldwide issue that necessitates international engagement. Africa and many developing countries lack the investigative power and technological capabilities to fully address this problem. Kenya and Rwanda are both affected by this worldwide issue. The issues that both countries face in combating cybercrime are strikingly similar. The only difference is how each country is preparing to meet these difficulties and what each has done so far to assist in the solution of this problem.

4.2 Counter Cybercrime Challenges Facing Kenya

In June 2013, the Kenyan government established a committee under the Communication Act of Kenya to spearhead efforts to combat cybercrime. The aforementioned Act declared war on cyber criminals, imposing harsh penalties for illegal cybercrime. In order

to ensure progress the purpose of the Act was to safeguard the government of Kenya within the entire system of ICT as the engine for electronic commerce and electronic governance. However, advances in technology and virtual communication have occasioned a protracted upsurge in the emergence of cybercrime criminal activities in the country as well as the introduction of a new trend of insecurity.⁷³

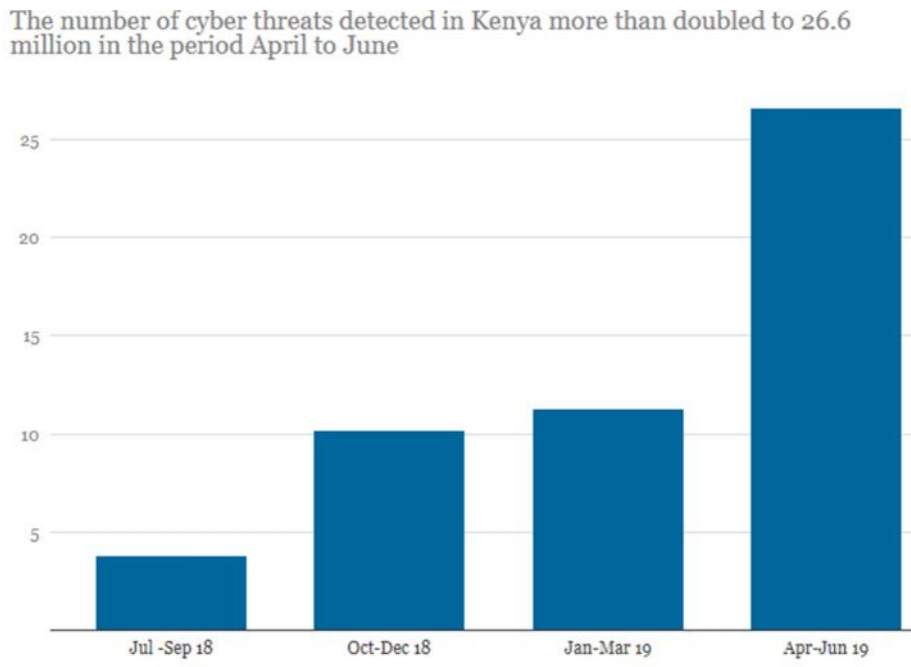


Figure 4.1: The number of cyber threats detected in Kenya more than doubled to 26.6 million in the period April to June

The accompanying bar chart depicts the increase in cybercrime from July 2018 to July 2019. Kenyan cybercrime incidents increased by 22.2 million within one year from 4.4 million to 26.6 million. As the country's commercial processes become more digitalized,

⁷³Longe, O and Chiemeké, S. Cybercrime and criminality in Nigeria – What roles is internet access points in playing? *Eur. Journal. Soc. Science.* 6(2008):133-139.

cybercriminals' potential threats grow and become more complicated. The expansion of the internet and increased access to cyber skills has created new opportunities for those involved in illicit activities as well as new job and commercial opportunities.

4.2.1 Challenges of Legislation

Any developing country faces a significant challenge in successfully completing the legal reform process, from initial recognition of a problem to the preparation of draft legislation, as well as its endorsement by national political institutions and implementation in a way that has a real impact on business and administrative attitudes and practices.⁷⁴ Inadequate legislation and the ineffectiveness of the same when there are already regulations in place have impeded the fight against cybercrime.⁷⁵ The bill of rights in chapter four of the constitution of Kenya, as the supreme source of law of the state, recognizes fundamental human rights, which are constantly a target for cyber thieves. This criminals infringe on individuals' Privacy, protection against individuals' communication, unlawful access to information, consumer protection rights, fair administrative action, access to justice and fair hearing, freedom of conscience, religion, and opinion, freedom of expression, and freedom of the media are just a few of the rights at the center of infringement. The Kenya Information and Communication Act 17 contain only a few parts that deal with cybercrime in the country, and they largely deal with electronic and mobile transactions, which is the main concern with Kenyan legislation. The agreement on cybercrime does not include a

⁷⁴ United Nations Conference on Trade and Development, Harmonizing Cyber laws and Regulations, the experience of East African Community, August 2013

⁷⁵ Ajayi, E. F. G. Challenges to enforcement of cyber-crimes laws and policy, Journal of Internet and Information Systems, School of Law, Kenyatta University, Nairobi, Kenya. 25 July, 2

thorough procedural law, which supports suspicions that the law was not drafted with the contemporary dynamics of cybercrime in mind.

4.2.2 Interested Parties Challenge

Interested parties and the Law Society of Kenya (LSK) have repeatedly thwarted efforts to declare illegal sections of the Republic of Kenya 2018 Act on Computer Misuse and Cybercrimes. The attorneys' group went on to sue the National Assembly, and the following institutions on allegations that the parts of the above stated Act would restrict media freedom and freedom of expression; the Attorney General, the Director of Public Prosecutions, and the Inspector General of Police.

The Law Society of Kenya contended that enforcing vague rules jeopardized the Bill of Rights by resulting in unconstitutional arrests and prosecutions.⁷⁶ The right to freedom of expression, access to information, and media freedom guaranteed by Article 19 of the Universal Declaration of Human Rights were jeopardized by the Computer Misuse and Cybercrimes Act 2018 according to the LSK. Sections this Act were deemed illegal and invalid by the LSK.⁷⁷ Geoffrey Maina, in collaboration with the Kenya Bloggers Association, was the first to file a petition to have the cybercrimes statute declared unconstitutional. Such interferences cause cases to stall in courts of law and at the inquiry level, depriving cybercrime victims of justice.

⁷⁶ Law society of Kenya versus the Attorney general of Kenya and four others, LSK Challenges Constitutionality of the Computer Misuse and Cybercrimes Act, June 2018

⁷⁷ Ibid

4.2.3 Challenge of Jurisdiction

Jurisdiction is another significant obstacle to the enforcement of cybercrime legislation. Each nation-state in the world must be able to adopt binding laws on all things and people within its borders without interference from the outside world; this is according to the demand by principles of state autonomy, sovereignty, and territorial integrity. That is why laws on the same issue in various independent nation states are made in different ways resulting in inexorable conflict of laws. As an independent country, Kenya may not allow a crime committed against it by another country to be punished outside its borders.

Each trial is predicated on the issue of jurisdiction; otherwise, any subject before the courts of law becomes basic to the issue of jurisdiction. If a court lacks the principle of jurisdiction, it is immediately devoid of the authority to hear the matter.

When a court's verdict is required to be imposed outside of the set boundaries, its extraterritorial competence becomes important. In terms of enforcing cybercrime laws, there are essentially two concerns that revolve around the subject of jurisdiction: geographical jurisdiction and jurisdiction in "personam."⁷⁸

Jurisdiction in personam allows a court of law to hear and decide a case of cybercrime that is of a nature but not within its jurisdiction. Unlike old-fashioned native crimes perpetrated in a precise location and the consequences felt by the victim(s) inside the same locality, cybercrimes are unique in nature and belong to their own category. In summary,

⁷⁸ Ibidem

where a clearly known cybercriminal is located in a territory other than the victim's locale, jurisdictional enforcement of cybercrime laws and regulations is a challenge. For the reason that the adjudicating court lacks geographical jurisdiction, it is unable to consider such a case competently. These occur when a criminal from another nation, such as Nigeria, uses the internet to commit a crime in Kenya. The victim is in Kenya, while the perpetrator is in Nigeria in this situation.

The issue of jurisdiction involves determining the extent to which a country can claim authority over external evidence, alien nationals, and distant land, as well as which country has legal grounds to prosecute suspects and sentence those responsible for cybercrime. In the event that more than one country possesses competent jurisdiction to try the case, which country will be given priority in hearing the case, and to what extent can anyone claim extraterritorial procedural jurisdiction? Because cyber jurisdiction is so far removed from traditional convention limits, many countries lack specialized legislation. As a result, such governments mostly rely on traditional geographical boundaries to determine whether or not they have jurisdiction over cybercrime.

4.2.4 Challenge of Extradition Processes

Extradition is the procedure by which a suspect accused of committing a crime by one legal authority is returned to the nation where the crime was committed for prosecution or punishment by a different legal authority. Alternatively, the surrender to judicial procedures of a person suspected of committing an infraction in another country.⁷⁹

⁷⁹ Oxford Dictionary of Law, 2002

However, according to the idea of state independence and sovereignty, things are different in practice. There is no provision that requires sovereign governments under international law to automatically repatriate cybercriminals for trial in the country where the crime was committed. As a result, nations where cybercriminals are domiciled frequently fail to return cybercriminals to requesting countries for various reasons, posing a barrier to the universal implementation of cybercrime laws. State sovereignty is one of the most significant obstacles to extradition of criminals to requesting states, which is often raised by countries to deny repatriation, particularly when the requested state has authority to try such criminals who are their nationals.

The Principle of Double Criminality is another significant impediment to extradition. This premise is acceptable when the crime is punishable under the laws of the requesting and harboring states. Some states' extradition laws provide a list of extraditable offenses, as well as a list of extraditable crimes for which repatriation is possible in order to meet this need.

For the purpose of deportation, the Extradition Act of 1962 has been applied to all crimes registered in the Second Schedule to the Act. The list includes all extradition cases with Commonwealth countries and those with which India has no treaty but mutuality. In the event of an accord with any state, a list of extraditable crimes is affixed, and extradition will be limited to those offenses entirely. If the crime isn't listed in the agreement, extradition will be tricky. To get around this challenge, states will sometimes include a

general section in the treaty covering extraditable crimes with a minimum consequence under both States' laws.

4.2.5 Challenge of Lack of Awareness of Cybercrime

The number of stakeholders actively involved in national internet governance is relatively modest. Despite the fact that Kenya has transitioned from a national to a decentralized style of governance, the bulk of the population significantly involved in the administration of the country are based in Nairobi. Due to a absence of understanding or cognizance, county managements are not ranking internet issues highly. Ordinary internet users and clients are merely concerned with the end product, namely access to the internet, and are either ignorant of or indifferent with the governance component. For there is a predisposition to cogitate internet governance as a technical subject, the discussion on internet policy and strategy entices primarily cyber specialists. "Businesses are hesitant to join the internet governance community, and as a result, they are unlikely to participate in or be aware of government initiatives involving the internet."⁸⁰ This could be due to the fact that firms are profit-driven and hence fail to notice the good in their procedures. The majority of businesses may be unaware of or uninterested in internet governance issues; they are preoccupied with their work and profiting from the internet. The difficulty is in convincing people that every person who uses the internet is a partaker in internet control.

The media rarely participates in end-user lobbying, but it does report on internet policy disputes on occasion. Except for the Kenya Human Rights Commission, which has

⁸⁰ Ibidem

recently begun active participation in internet governance issues, most mainstream non-governmental organizations (NGOs) have not been involved in internet governance disputes. "This is mostly due to a lack of real awareness among NGOs of the link between the internet and human rights," says the report.⁸¹

4.2.6 Challenge of Anonymity of Criminals

The anonymity of hackers is one of the most difficult aspects of combating cybercrime in Kenya. The global information system is open to all without any prerequisites that must be met before a user can communicate with anyone anywhere in the world making it a challenge to identifying prospective cybercrime suspects.⁸² Cybercriminals can mask their identity using various communications devices, making it problematic to trace the online Internet Protocol (IP) address of any user, thanks to the unrestricted freedom of information and communication. The subsequent obstacle would be a cybercriminal's distinctiveness, which is camouflaged from the proprietor or operator of the Internet service provider and from law implementation in the event that a cybercriminal's IP address is traced to a specific location. Several telecommunications devices include Siphons and Tor (The Onion Router). Guard Internet users' identities and hackers' communications from being easily traced even if the laws were perfect, no case could be effectively prosecuted in this circumstance.

⁸¹The Internet Legislative and Policy Environment in Kenya report January, 2014

⁸² Ajayi, E. F. G. Challenges to enforcement of cyber-crimes laws and policy, Journal of Internet and Information Systems, School of Law, Kenyatta University, Nairobi, Kenya. 25 July, 2016

A foundational concept of law is that "you cannot set something on nothing and expect it to stand." No law, no matter how well-crafted or envisioned, can work as long as cybercriminals' identities remain ambiguous since there is no law that works in a vacuum, which is the point being stressed here. "Cybercrime laws were primarily enacted to apprehend and prosecute cybercriminals; yet, if the criminals are not traceable, any law(s) enacted is a waste of time."⁸³ Since people still do not use their identity documents to register their cellphone lines, the push to remove anonymity in the use of the Internet in Kenya has not been as successful.

4.2.7 Challenges of Investigation and Prosecutions

This is evidenced by law enforcement agents' insufficient awareness of information and technology concerns related to cybercrime, who rely on investigative procedures used to deal with traditional crimes. This dilemma is strongly linked to the issue of digital evidence processing, which Kenya severely lacks due to the lack of an improved digital forensic laboratory to cope with this sophisticated and dynamic crime. Kenya, as a developing country, faces the challenge of losing evidence needed to continue an investigation and prosecution owing to inadequate storage. In Kenya, prosecutions are based on physical evidence, but electronic evidence is subject to rigorous controls, making convictions difficult.

The inconsistency in the law has made it difficult for the prosecution to prove charges beyond a reasonable doubt, which is the legal standard in Kenya. Another hurdle to the

⁸³ Ibidem

implementation of cybercrime legislation, wherever it is attempted, is the nature of evidence in possession by the prosecution and its acceptability in the course of a cybercriminal hearing. The prosecution must establish their case beyond a reasonable doubt in order to gain a conviction of the accused. Unfortunately, in many situations, the available evidence to be relied on by prosecutors is suspect, and most attempts to bring cybercriminals to justice are unsuccessful.

The simple act of turning on and off the computer might affect critical evidence connected with time and date recordings of the incidents, causing significant challenges in locating and safeguarding electronic evidence. A key difficulty in investigation and prosecution is searching through huge amounts of data in order to recognize information required, as well as the annexation of digital evidence from hard drives on networked computers containing both appropriate and inappropriate content. A significant barrier is presented by having to decide which material is relevant to the charges in question and imaging hard drives, causing issues with search warrants including non-specified data on hard drives. This could lead to the entire search and seizure operation being inaccurate. It's nearly impossible to sort through 80 GB of material on a hard drive to figure out what's relevant to the case at hand.

Another issue is disabling networks when seizing data, which is particularly problematic for huge public and private organizations that heavily depend on network access 24 hours daily, and the problem of the culprit tidying away data externally on other computer

storage in order to evade detection.⁸⁴ Due to the transnational nature of cybercrime, conducting investigations across international borders creates numerous challenges that cause delays and increased expenditures. Teleconferences can be difficult to arrange for all parties involved, especially if they are required for diplomatic purposes. Documents must often be translated, which is costly and delays investigations.

Different states have assigned varying degrees of prominence to cybercrime investigations. For the states in which violent crime is rampant or where the countries national interests are at risk, economic crimes executed using computers are normally at the bottom of the significance list. As a result, requests for cooperation in cybercrime cases are given considerably lesser precedence, particularly if they are initiated by country with no history of collaboration.

4.2.8 Challenges of Cooperation

"Bilateral and multilateral treaties and agreements more widely entrench access to digital evidence and formal international cooperation on cybercrime."⁸⁵ These instruments that have an influence on the freedom of a nation-state generate limitations for the process and conduct of foreign law implementation and inquiries. There are a number of challenges that hinder collaboration and effectiveness notwithstanding the fact that a number of bilateral and multilateral cooperation mechanisms have been put in place. Treaties are frequently utilized for mutual legal aid in order to facilitate international criminal

⁸⁴Dr Russell G. Smith, Investigating Cyber Crime: Barriers and Solution, Pacific Rim Fraud Conference, 2003

⁸⁵ Allison Peters and Amy Jordan, Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime, Report Published October 2, 2019

investigations by giving legal support for authorities from other nations. This type of mechanism covers an extensive range of services, comprising the identity and locality of people, the service document, the obtaining of evidence, goods, and documents, the execution of search and seizure requests, and aid with proceeds of crime. However, there are a number of issues associated with the use of mutual legal assistance agreements.

The main issue is that official requests are delayed and inconvenient. Direct sending of documents is challenging because it can only be done in an emergency and to a law court or tribunal hearing the case. Direct appeals for help are also problematic to use unless the individual looking for aid knows precisely to whom the request should be made. The side offering aid endures the costs of mutual assistance, which causes hardship for less developed countries to bear because they are expected to process a significant number of requests for assistance from major countries but rarely seek assistance themselves.

"Obtaining aid in cybercrime cases through official assistance agreements between states can be extremely time-consuming and unsuccessful."⁸⁶ Searches must regularly be conducted immediately in order to preserve evidence housed on servers, but the idea of having to wait weeks or even months for sanctioned consular channels to be followed is discouraging. Most African states have not joined the Budapest Convention, a well-known vehicle for tougher and more uniform legislation, making cooperation difficult.

⁸⁶Dr. Russel G. Smith, 'Investigating Cybercrime: Barrier and Solution, Pacific Rim Fraud Conference, 2003

4.2.9 Challenges of Costs and Time

Because forensic evidence is required in the prosecution of cybercrimes, the price of doing so as a technical crime resolving strategy is substantial compared to gathering evidence in conventional crimes. It is very costly to carry out cybercrime investigations because of the high-tech equipment, materials, and knowledge required in conducting such investigations. Many complications arise when a criminal is wanted extraterritorially, resulting in increased costs in the cybercrime investigation. These include road, water and air travel where it is necessary for investigators to be physically present in another jurisdiction where the offence was committed, telephone or cellphone conversation and Tele-conferences where this is not necessary, this is because investigators must interact with other jurisdictions in order to successfully corroborate efforts to disentangle cybercrime. It should be emphasized that such interactions by investigators are problematic owing to time variances; for example, when some Americans are sleeping, Kenyans may be working. Extra expenses related with travel include food, accommodation, transportation, entertainment, and other accompanying expenses.

4.2.10 Challenges of Current Policies

Kenya is still in the initial stages of developing a all-inclusive and multi-stakeholder consultation agenda for cybercrime policy. The respective bodies and mechanisms must be harmonized to guarantee that the resultant cybercrime policy and legal environment is favorable to the approvals of human rights approaches to cyber security. "In the cyber security area, discussion and activities are divided, with an insufficient focus on

cybercrime."⁸⁷ This jeopardizes Kenya's drive for a comprehensive method to effectively oversee and govern the Internet. Several issues in the domain of policy framework have hampered the enforcement of cyber security regulations. "Inadequate skills in the cyber security sector, insufficient cognizance of cyber security issues among various stakeholders, lack of conducive legal framework and absence of related recognized infrastructure for Information Communication and Technology development and application, and inadequate supervisory capacity, particularly in the face of the convergence of lack of specific and effective legislative mechanisms on privacy, security, cybercrime, ethical and moral conduct, encryption, digital signatures, copyrights, intellectual property rights, and fair trade practices; lack of a culture that fosters the adoption of internet security standards in various sectors; lack of specific and effective legislative mechanisms on privacy, security, cybercrime, ethical and moral conduct, encryption, digital signatures, copyrights, intellectual property rights, and fair trade practices."⁸⁸

In Kenya, civil society organizations are thought to be underrepresented. The state recognizes civil society and multi-stakeholder engagement, albeit the state's facilitative methods and structures are unclear. The ostensible absence of a methodical process for endorsing cyber policies and legislative frameworks has resulted in a disjointed policy process. For example, the cyber security regulations came first before the computer and cybercrimes bill, which was then unveiled shortly after the draft National ICT Policy. In

⁸⁷ Nanjira Sambuli, etal, Global Partners Digital, Mapping the Cyber Policy Land Scape: Kenya, November 2016

⁸⁸ Ibidem

addition to the existing bills and policy review process, the Senate recently introduced the Cyber Security and Data Protection Bill (2016) as a rationale or motivation. "This duplication of resources and lack of coordination endangers the country's ability to implement sustainable legal frameworks." This is, however, a publicly recognized problem that the government is eager to address."⁸⁹

4.2.11 Challenge of Dynamic Sophistication

Data is the illicit commodity in a self-sufficient and sophisticated digital hidden economy. Individual and fiscal data gotten unlawfully and used to achieve admittance to prevailing bank accounts and credit cards, or to find new lines of credit under deception, has a financial price. Attempting to obtain information such as usernames, passwords, and credit card details, and sometimes, indirectly, money, by individuals concealed as a trustworthy entity in an electronic communication (Phishing) and attempting to obtain information such as usernames, passwords, and credit card details, and sometimes, indirectly, money, by camouflaging as a trustworthy entity in an electronic communication (pharming)⁹⁰. Malware dissemination and business data hacking are reinforced by a full-fledged infrastructure of malevolent code writers, expert web hosts, and individuals who may rent networks of thousands of corrupted computers to carry out computerized attacks.

⁸⁹ Ibidem

⁹⁰GuhaDigijah, Cybercrimes , Challenges and Solutions, International Journal of Computer Science and Information Technologies, volume 4, September 2013

4.2.12 Challenge of Changing Cyber Technology

As never before in human history, society's "information" and improvements in communications technologies have collided. This collision has enhanced the blowout of a kind of crime concentrated on the commodity of individual information, which moves much too rapidly for old-style law enforcement methods to keep pace with. A large number of computers compromised every day, and the scope of the problem puts the authorities' capability to respond in danger. Cybercrime proportions continue to rise in tandem with the Internet embracing, mobile internet access, and the continued positioning of broadband internet infrastructure throughout the country, with potential victims staying online for longer periods of time and capable of transmitting much more data than before. This presents new heights of susceptibility; with probable victims online for longer periods of time and capable of handling much more data than earlier.

4.2.13 Challenge of Inadequate Training of Law Enforcers

Investigations may yield little or no results at all even with strong applicable and procedural domestic criminal laws and consent to international conventions unless law enforcement officials are highly trained, properly equipped, and competent enough. The criminal justice community faces a tremendous challenge in communicating a common understanding of the essential technological skills, knowledge, and roles done during investigations and convictions of cybercriminals. Cybercriminals are continually stocking up on the latest recent computer software. Their knowledge cannot be compared to that of law enforcement agencies, which are government employees that are undertrained,

underpaid, and perform their duties with little enthusiasm. Cybercriminals, on the other hand, become experts in computer and internet concerns.

The availability of finances for study and operations by law enforcement authorities is another consideration. Cybercriminals, on the other hand, have a leg up on law enforcement organizations in terms of resource availability and crucial computer and cyberspace abilities. Even if law enforcement agencies did an excellent job investigating cybercrime, it is a truth that, during the litigation stage, prosecution attorneys' competence is still critical in securing a cybercriminal's conviction since the prosecution must prove its case beyond a reasonable doubt. Unfortunately, there aren't enough savvy prosecutors in the office of deputy public prosecution to effectively pursue cybercriminals. Cybercriminals, on the other hand, have unrestricted access to renowned private attorneys who specialize in cybercrime. Apart from the technicalities in cybercrime trials, cybercriminals have sufficient money to pay top-notch attorneys to defend them during the hearing of their criminal cases.

4.3 Counter Cybercrime Challenges Facing Rwanda

The Republic of Rwanda is an East African country located in East Central Africa and borders the Democratic Republic of Congo to the West, Uganda to the North, Tanzania to the East, and Burundi to the South. In recent years, Rwanda's access to information and communication technologies (ICTs) has vastly improved. In 2017, the International Telecommunication Union (ITU) stated that 70% of the population had mobile subscriptions, with 20% of those having active mobile broadband connections. The

advancement of digital interactions and the development of Information Communication Technologies (ICT) created new opportunities and opened up new windows, resulting in the advent of new forms of criminal activity.⁹¹ The use of ICT improves the effectiveness and efficiency of criminal actions that take place in the real world by providing new and enhanced opportunities to commit crime. Due to the following issues, Rwanda, like many other countries throughout the world, has struggled to combat cybercrime:

4.3.1 Challenges of Legislation

Although Rwandan criminal law did not recognize the word "cybercrime," it was expanded to allow for the arrest and successful prosecution of cyber offenders. As a result, the lack of suitable regulations and procedures makes it difficult to investigate and prosecute cybercriminals. Legislation, particularly the modernization of substantive and procedural regulations on what constitutes illegal activity in cyberspace and a sufficient legal framework for its investigation, necessitates a long-term commitment.⁹² The lack of suitable rules and processes that govern in diverse jurisdictions impeded Rwanda's efforts to investigate and prosecute cyber offenders.

The only laws in Rwanda that dealt with cybercrime were the Organic Law N001/2012/OL of 02/05/2012 creating the penal code and Law N02/2016 of 18/06/2016 regulating information and communication technologies. While these rules governed some computer-related activities, they lacked a legal foundation for the prevention and

⁹¹Stavrou Aki. 2000, *Mission Impossible: E-security in South Africa's Commercial and Financial Sectors*, Institute for Security Studies, Pretoria

⁹²Newburn, T., (2008), *Handbook of Policing*, 2nd ed. William publishing, Devon

prosecution of computer-related offenses. Rwanda established a cybercrime law to help protect private and government information and infrastructure from cybercrime and cyber-attacks in order to close this gap.

Other challenges in combating cybercrime in Rwanda include a deficiency of cyber security and information security consciousness, a lack of adequate knowledge and skills in the area of cyber security and cybercrime investigations, a lack of consciousness about cyber laws and regulations at both corporate and individual levels, high-level information, communications technology, and emerging technology, and a lack of high-level information, communications technology, and emerging technology. The other challenge is unknown victims, difficulty detecting and identifying perpetrators across borders, and a lack of cyber security officers' training.⁹³

4.3.2 Challenges of Jurisdiction

The biggest distinguishing element of cybercrime from regular crime is its lack of boundaries and anonymity. Cybercrime crosses all lines and has no regard for borders. The challenge of applying laws to illegal activity beyond geographical boundaries continues to be a source of worry. Cybercrime is on the rise across states, regions, and the planet as a whole, thanks to unstoppable technology. "The application of laws to criminal activity across geographical boundaries" remains a challenge for countries.⁹⁴ For detachable elements in several locations, it is extremely difficult for detectives to gain a true picture of the entire crime process.

⁹³ Mugisha, David, Annual INTERPA Conference, Methods to Combat Cybercrimes in Rwanda, 2019

⁹⁴ Ibidem

4.3.3 Challenges of Cyber Security and Information Awareness

Ordinary internet users and consumers in Rwanda, like many other developing nations, are primarily interested in the end user product, which is internet connection, and are either unaware of or unconcerned about the governance side of things. Furthermore, there is a tendency to regard internet governance as a government prerogative, with regular citizens having no say in the matter. Professionals in this realm of expertise are drawn to internet dogma dialogues. Criminals in Rwanda have easy access to sensitive information due to a lack of computer or password security. As a result, thieves frequently take advantage of lax security methods to get access to computers and steal data in order to carry out their illicit activities.

4.3.4 Challenges of Expertise and Skills in Cybercrime Investigations

Insufficient investigations are hampered by a lack of analytical and technical capability. Officers assigned to cybercrime investigations must have appropriate qualifications, knowledge, and skills. Ninety-seven percent of all high-tech crimes are estimated to go uncovered. According to Heredion, Rwanda had high ambitions and aimed to become a knowledge-based, technology-led economy by 2020, aided by Rwanda's transformation into a regional information, communication, and technology powerhouse.⁹⁵ The National Information and Communications Infrastructure Plans, as well as the National Policy on Science, Technology, and Innovation, are two main ways to implementing information, communication, and technology in Rwanda.

⁹⁵Ndayisabye H,2011, Cybercrimes in Rwanda, An Investigative case study of pirating in Nyarungenge District, 2005-2010

"Cybercriminals are ignorant treasure hunters who are always looking for ways to make unlawful riches or, in rare situations, cause computer system harm; they have been characterized as professional thieves and fortune soldiers."⁹⁶ The expertise of cybercriminals, who are experts in computer and cyberspace issues, cannot be compared to that of law enforcement agencies, which are merely government employees who are poorly trained, underpaid, and provide services without enough security and protection. Cybercriminals are far ahead of law enforcement authorities in terms of access to funds and the requisite development of computer and related skills.⁹⁷ As a result, initiatives aimed at investigating and enforcing cybercrime laws are underdeveloped.

4.3.5 Challenges of Locating and Identifying Perpetrators

It is not easy to track down and identify the perpetrators. It's hard to know who's doing what at any one time or where the internet user is at any given moment. The worldwide information structure is open to anyone, and has no strict requirements to meet before connecting with anyone anywhere on the planet, making it simple for internet users to log in and join. In this situation, cyber criminals take advantage of the unlimited access to information and communication, enabling them to hide their personality by engaging various telecommunications strategies to make it problematic to be identified by any users' online Internet Protocol (IP) address.

⁹⁶ Legal Brief E Law & Management Cyber law & Technology Watch Issue No: 1581 29th 2015

⁹⁷ Ajayi, E. F. G. Challenges to enforcement of cyber-crimes laws and policy, Journal of Internet and Information Systems, School of Law, Kenyatta University, Nairobi, Kenya. 25 July, 2016

4.3.6 Challenges of Dynamic Technology

Another issue in Rwanda's fight against cybercrime is the apparent implications of the new information and communications revolution. As a result, an unprecedented number of information-based products have been created and disseminated, forcing traditional views of crime and criminality to be re-examined. Individuals, public and private organizations, the economy, and society as a whole face a number of issues as a result of digital era crime.

4.4 Secondary Data Analysis

Cybercrime is a worldwide issue that necessitates international response. Several underdeveloped countries lack the investigative and technological capacity needed to effectively address the problem. Kenya and Rwanda are both affected by this worldwide issue. As previously said, there are numerous similarities in the issues encountered by the two countries in combating cybercrime. The only difference is how each country is preparing to meet these difficulties and what each has done so far to assist in the solution of this problem.

4.4.1 Kenyan Approach to Counter Cybercrime

The Communications Authority of Kenya (CA) was obliged by the Kenya Information and Communications Act of 1998 to build a national cyber security management framework.⁹⁸ The Kenyan government established a multi-agency collaboration framework known as the National Kenya Computer Incident Response Team

⁹⁸The Kenya Information and Communications Act, 1998

Coordination Centre (NKE-CIRT/CC) in order to mitigate cyber threats and foster a safer Kenyan cyberspace. This multi-agency collaboration is responsible for the national coordination of cyber security as Kenya's national point of contact on cyber security matters, in accordance with the provisions of the Kenya Information and Communications Act.

The 2018 Act on Computer Misuse and Cyber Crimes is one of the significant features that supports national cyber security pliability and has gone a long way toward augmenting the multi-agency cooperation framework. Cybercrime in Kenya is also covered by a number of laws, including Article 31 of Kenya's 2010 Constitution, the Kenya Information and Communication Act No. 5 of 2018, and the Data Protection Act No. 24 of 2019. The vast and dynamic nature of ICT has resulted in a diverse set of issues.

The Government of Kenya (GoK) has taken steps to solve these concerns by ensuring national cyber security, promoting economic progress, and safeguarding citizens' interests. Kenya.⁹⁹ The Government of Kenya took the first steps toward developing a cyber-security governance framework by entrusting regulatory responsibilities to the Communications Authority of Kenya (CAK) and establishing the National Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC), which serves as an important first step for national-level incident response. Kenya passed an Act of Parliament prohibiting unauthorized access to, use of, or meddling with a computer; protecting the veracity of computer systems and the secrecy, integrity, and availability of

⁹⁹ Ministry of Information Communication and Technology, National Cyber security Strategy report, 2014

data; preventing computer system abuse; facilitating the collection and use of electronic evidence; and other related purposes. To promote harmonized situational awareness and incident response, the GoK continues to refine its cyber security control model, define steady state and incident response roles and tasks, and expand KE-information CIRT's relationships across the Government of Kenya, with private sector associates within Kenya, and with regional and international partners.¹⁰⁰

Article 19 of The Kenya Cybercrime and Computer Related Crimes Bill in July 2014, evaluated the first draft of the Kenya Cybercrime and Computer Related Crimes Bill (referred to as Cybercrime Bill). The Bill's conformity with international and comparable standards for the protection of freedom of expression and the right to privacy was examined. The Office of the Director of Public Prosecutions (ODPP) introduced the bill in order to provide law implementation agencies with the required legal and forensic tools to counter cybercrime, which is stated to have cost the government over Kshs two billion (2 billion).¹⁰¹ The bill follows a June 2014 Cyber Security Conference, which proposed the establishment of a comprehensive cybercrime law in view of the present legal context's apparent limitations in dealing with recent terrorist incidents.¹⁰² However, critics contend that the draft Cybercrime Bill's treatment of "content-related" crimes falls well short of international standards on freedom of expression. The bill, in particular, has extremely wide speech offenses, which might have a severe impact on freedom of expression.

¹⁰⁰ Ibidem

¹⁰¹ Ibidem

¹⁰² The Cybercrime and Computer Related Crimes Bill, 2014.

Kenya's government ratified the Computer and Cyber Crime Act into law in May 2018, in response to hackers and high-profile cyber-attacks. This was to provide for computer system violations; to permit appropriate and effective detection, prohibition, prevention, response, investigation, and prosecution of computer and cybercrime; to facilitate international collaboration in dealing with computer and cybercrime issues; and for other related purposes.¹⁰³ Critics believe it was an odd move because law already exists that addresses these issues. The Kenya Information Communication Act, as well as the Penal Code and its regulations, have already made some cybercrimes illegal. For example, it could have been altered to raise the penalty for specific offenses, but the Computer and Cyber Crime Act has replaced its provisions.

¹⁰³ Kenya Gazette Supplement Acts, 2018, The Computer Misuse and Cybercrimes Act, No. 5 of 2018

4.4.2 Rwanda's Approach to Counter Cybercrime

RWANDA NATIONAL CYBER SECURITY GOVERNANCE FRAMEWORK

2015-2020

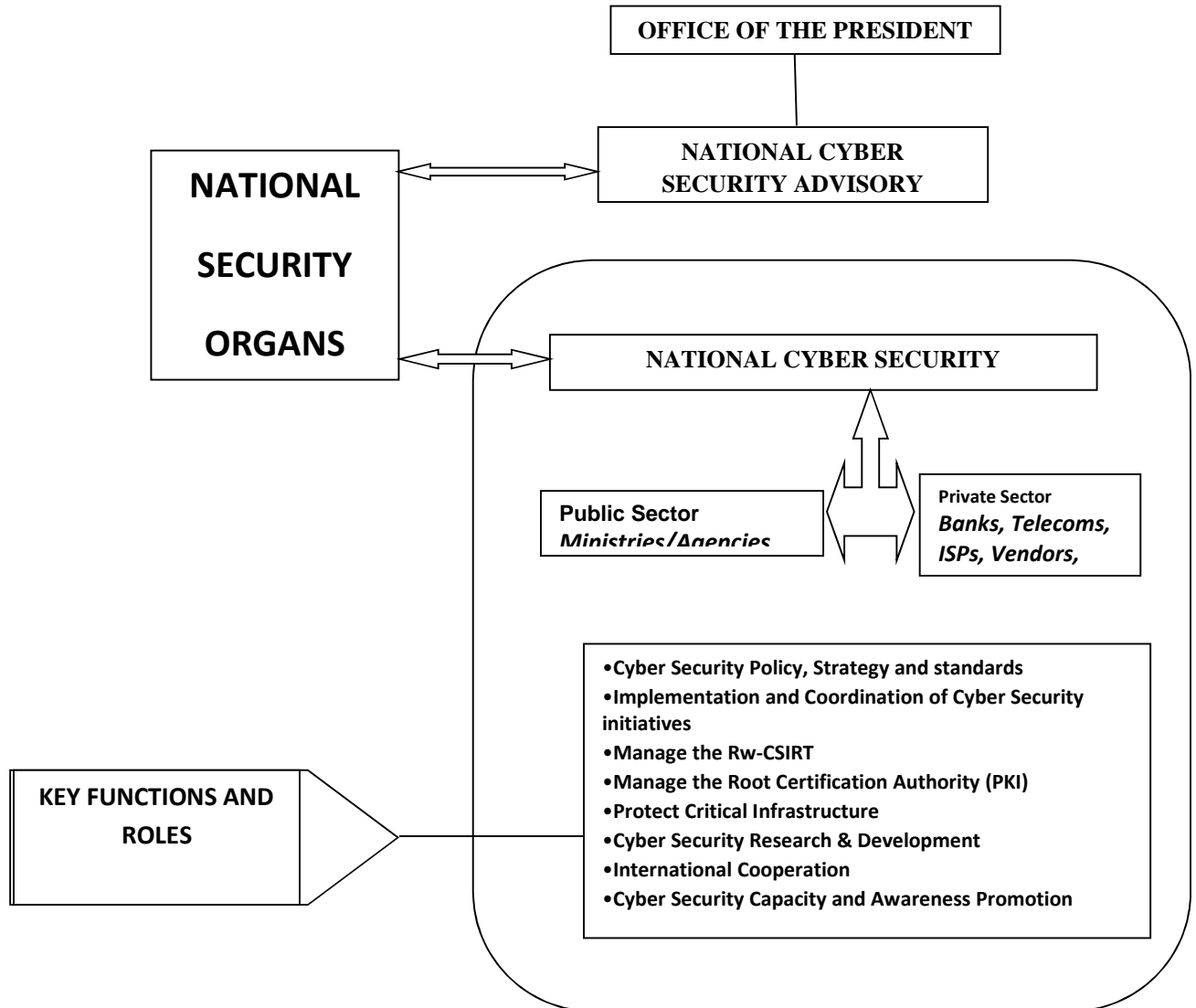


Figure 4.2: Methods and implementation to combat cyber-crimes in Rwanda,

February 2019

In Rwanda, cyber security has progressed to the point that it is now considered an issue of national importance and is being addressed more seriously. Rwanda's National Cyber Security Policy was passed in 2014 to protect government information and infrastructure

from cyber-attacks, and implementation began in 2015. Rwanda created a three-million-dollar cyber security system in 2016 with the goal of protecting public and private institutions against internet crimes.¹⁰⁴ To coordinate the country's cyber security efforts and to prevent and respond to cyber security incidents and threats in public-private companies Rwanda formed the Computer Security and Incident Response Team (Rw-CSIRT). According to the Global Economic Crime and Fraud Survey 2018 Rwanda report, 56 percent of Rwandan respondents said they have a fully operational cyber-security program that involves both detection and prevention of cybercrime.

Beyond recognizing the concerns of cybercrime and cyber-attack, Rwandan players at all ranks and across many sectors began to communicate, plan, organize, and react to problems in near real time. Rwanda's national police, Rwandan investigative bureau, and national security agencies are developing cybercrime fighting capabilities and putting in place additional cyber security measures to combat cyber threats.¹⁰⁵ To raise awareness and minimize cyber risks, Rwanda collaborates with NGOs, public and commercial organizations, academia, and the media (television, radio, and newspaper firms) to build cyber security education and training institutes.

Rwanda opened a new forensic lab with a digital forensic department in 2018, which would aid in the gathering of evidence for civil and criminal matters, as well as interior matters at law firms of any size.¹⁰⁶ In 2015 Rwanda's government created a national cyber

¹⁰⁴ Rwanda: 2016 law governing information and communication Technologies, Legal analysis, may 2018

¹⁰⁵ Global Economic Survey 2018 (Rwanda Report)

¹⁰⁶ Ibidem

security policy to help protect government information and infrastructure from the increasing number of cyber-attacks.¹⁰⁷ Rwanda established a cybercrime law to close the gap, allowing private and government information and infrastructure to be protected from cybercrime and cyber-attacks. As the government considers imposing the cyber security department, dubbed "Cyber Battalion," Rwandan police have established a cybercrime squad, while the Ministry of Defense has allocated female troops to play a key role in the battle against cybercrime. Rwanda requested \$1.5 million to build a cyber-security center in Eastern Africa to coordinate investigations into cybercrime and cyber-enabled crimes such as terrorism, human trafficking, and money laundering.¹⁰⁸

4.5 Analysis of Primary Data

In this part, descriptive data from Kenya and Rwanda's primary sources is presented. Background information, response rate, primary issues facing counter-cybercrime, mitigating measures put in place by both countries, and what should be done to lessen the obstacles of counter-cybercrime are all included in this part.

The gender, position held/designation, degree of education, and duration of service of respondents were used to create the background information for this study.

¹⁰⁷ David Mugisha, *Methods and Implementation to Combat Cybercrimes in Rwanda*, February 2019

¹⁰⁸ *Ibidem*

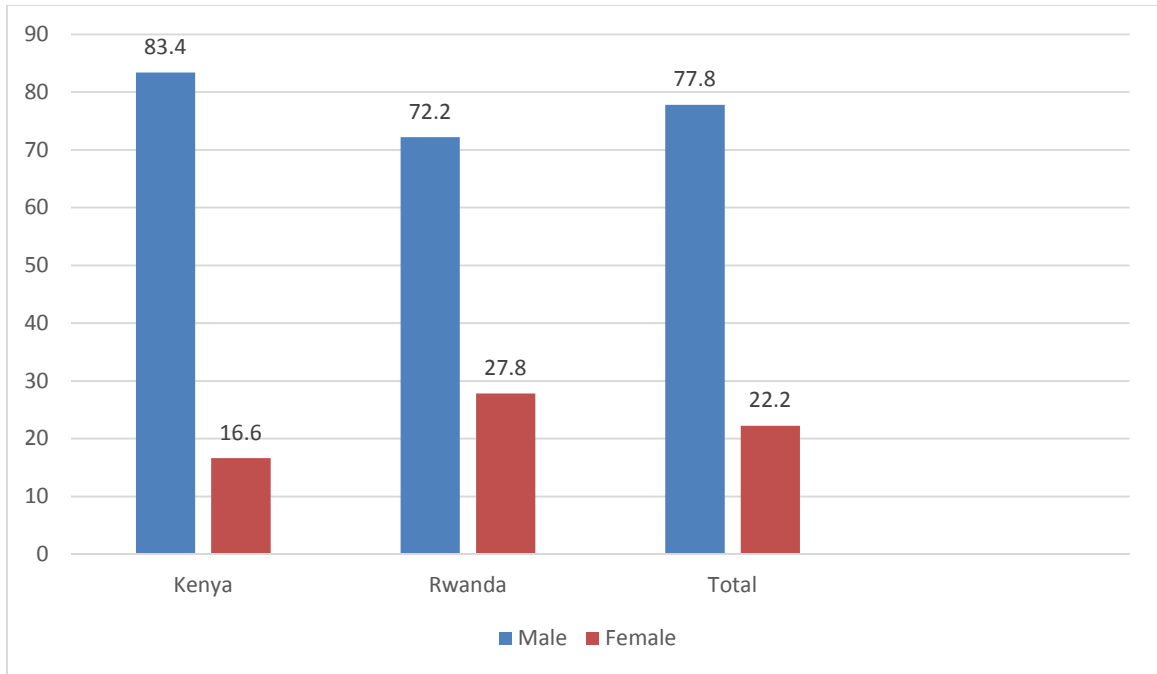


Figure 4.3: Gender presentation

According to the preceding graph, male respondents made up 77.8% in both countries, while female respondents made up 22.2 percent. This indicates that men are the majority of people dealing with counter-cybercrime issues. This accurately reflects the population of people who work in security-related fields. Male personnel outnumber female personnel in the majority of cases.

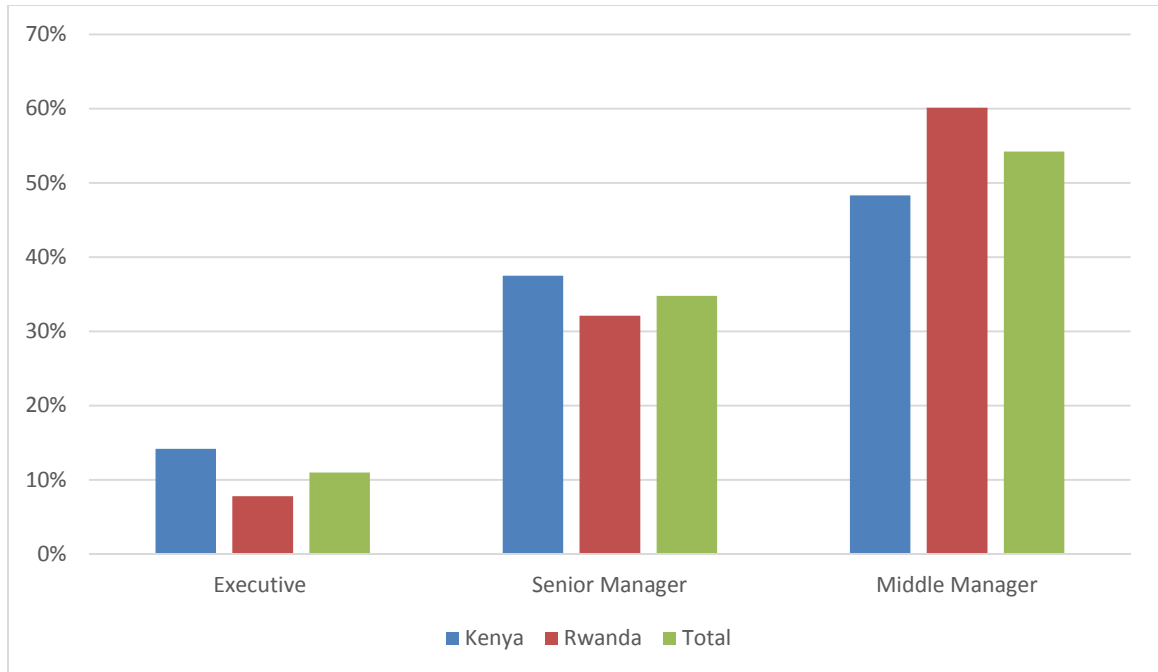


Figure 4.4: Position held/ designation

People in the middle management cadre in both countries are the ones who deal with counter-cybercrime concerns on a regular basis, as shown in Figure 4.4. For example, middle managers made up 48.3 percent of the total number of respondents in Kenya, whereas they made up 60.1 percent in Rwanda. Middle managers made up 54.2 percent of the total workforce in both nations. This group does not make decisions, which may explain why counter-cybercrime problems have received little attention.

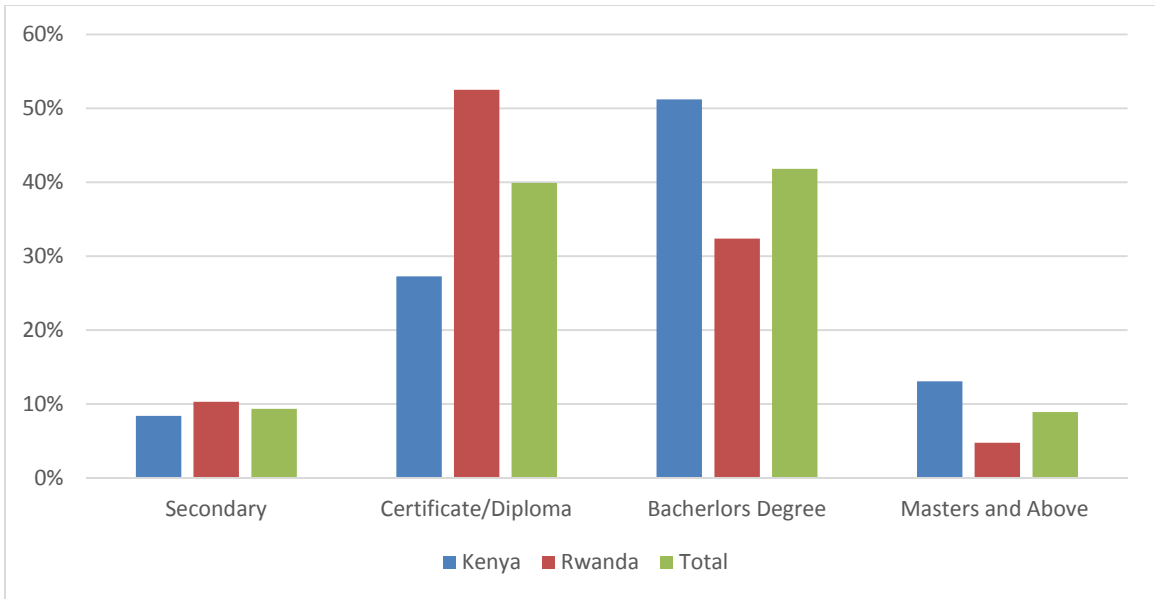


Figure 4.5: Level of education acquired by respondents

The majority of those involved in counter-cybercrime hold bachelor's degrees, diplomas, or certifications, as shown in Figure 4.5. In this survey, 41% of respondents had a bachelor's degree and 39% have diplomas and certifications. This is clear evidence that combating cybercrime necessitates more training beyond standard school credentials.

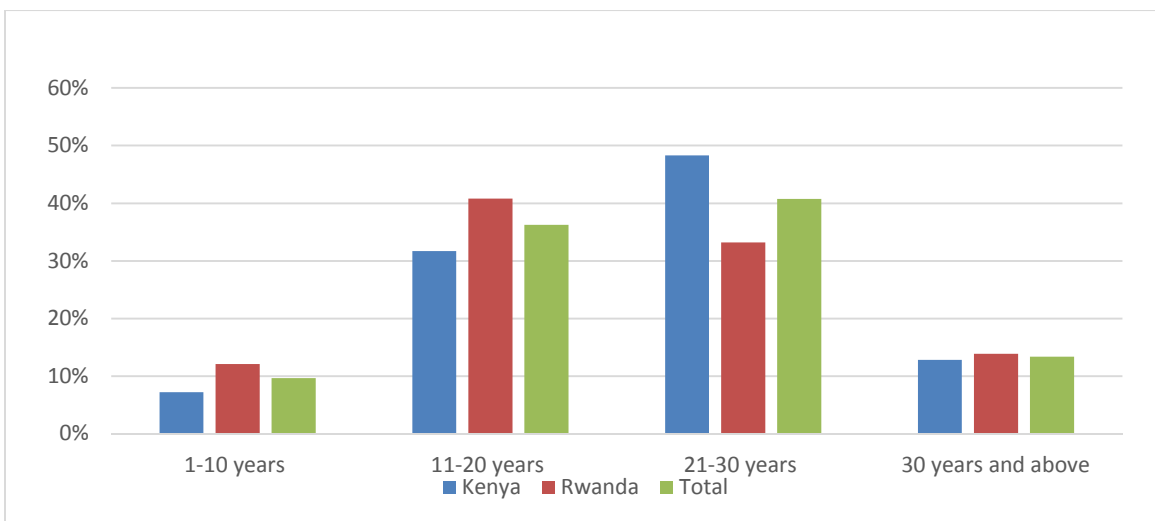


Figure 4.6: Length of service of respondents

As indicated in figure 4.6, the majority of the respondents have worked for 11 to 30 years. 40.75 percent have worked between 21 and 30 years, and 36.25 percent have worked for the period between 11 and 20 years. The total number of responses in these two categories is 77 percent. This demonstrates that the two groups have accumulated the necessary knowledge to combat cybercrime over time. On the other hand, 9.65 percent have only worked for 1-10 years and have little experience with counter-cybercrime difficulties. The other group is those who have worked for 31 years or more, which accounts for 13.35 percent of the total. This percentage is low since cybercrime is a relatively recent phenomenon, and many people in the older generation are unaware of it.

Table 4.1: Response rate

	Kenya		Rwanda		Total	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Response	62	82.7%	56	74.7%	118	78.7%
No response	13	17.3%	19	25.3%	32	21.3%
Total	75	100%	75	100%	150	100%

Respondents from the Kenyan and Rwandan defense forces, police services, directorates of criminal investigations, regional and national counter-terrorism centers, national intelligence services, information communication and technology, and the ministries of foreign affairs were given a total of 150 questionnaires. A total of 118 questionnaires were completed and returned correctly, while 32 respondents did not respond. As illustrated in figure 4.7, this response equates to an average of 78.7 percent. According to Maria (2018),

at least 70% of face-to-face surveys are acceptable, and this answer is sufficient to allow the researcher to generalize.

Table 4.2 Respondents opinion on whether counter cybercrime face challenges

	KENYA	RWANDA	TOTAL
Strongly agree	38.2%	30.1%	34.15%
Agree	52.1%	43.7%	47.9%
Disagree	7.4%	17.6%	12.5%
Strongly disagree	2.3%	8.6%	5.45%

Countering cybercrime in Kenya and Rwanda has a number of obstacles, as shown in the table above. According to the above table, 34.15 percent strongly agree, while 47.9 percent just agree that both Kenya and Rwanda face issues in combating cybercrime. As a result, solutions to the problem must be sought.

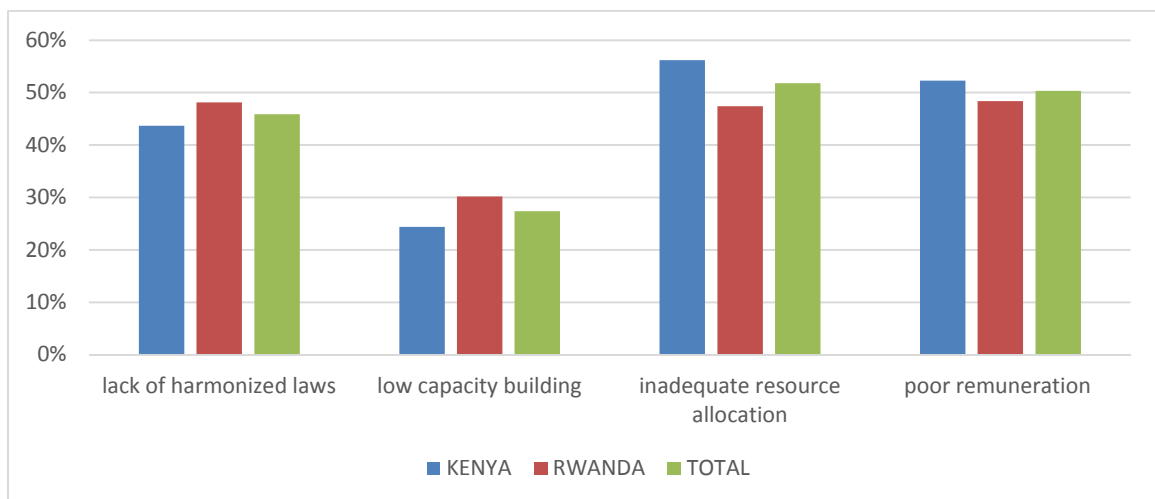


Figure 4.7: Some of the main challenges in counteracting cybercrime

Lack of unified regulations, limited capacity building, inadequate resource allocation, and poor remuneration are among the primary issues facing counter-cybercrime, as seen in the graph above.

According to the replies collected, the primary issue in both countries was insufficient budget allocation, followed by poor remuneration of personnel charged with combating cybercrime. The lack of harmonized laws to address counter-cybercrime concerns was the third issue, and insufficient capacity building was the fourth. In both countries of study, the issues listed above were identical.

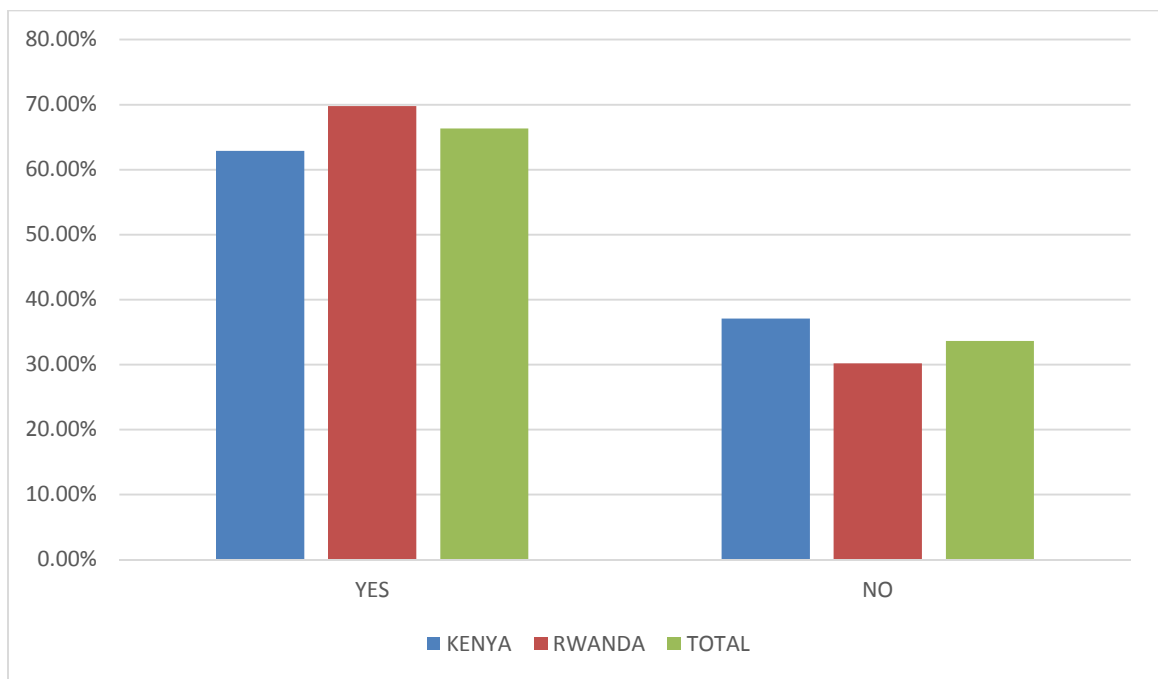


Figure 4.8: Opinions on difference in jurisdiction and countering cybercrime

According to the graph above, a total of 68,7% of respondents agreed that varied jurisdictions presented a challenge in combating cybercrime. Because what constitutes a

cybercrime offense in one nation may not be a crime in another, the host country may refuse to extradite a criminal to face cybercrime charges in a different country.

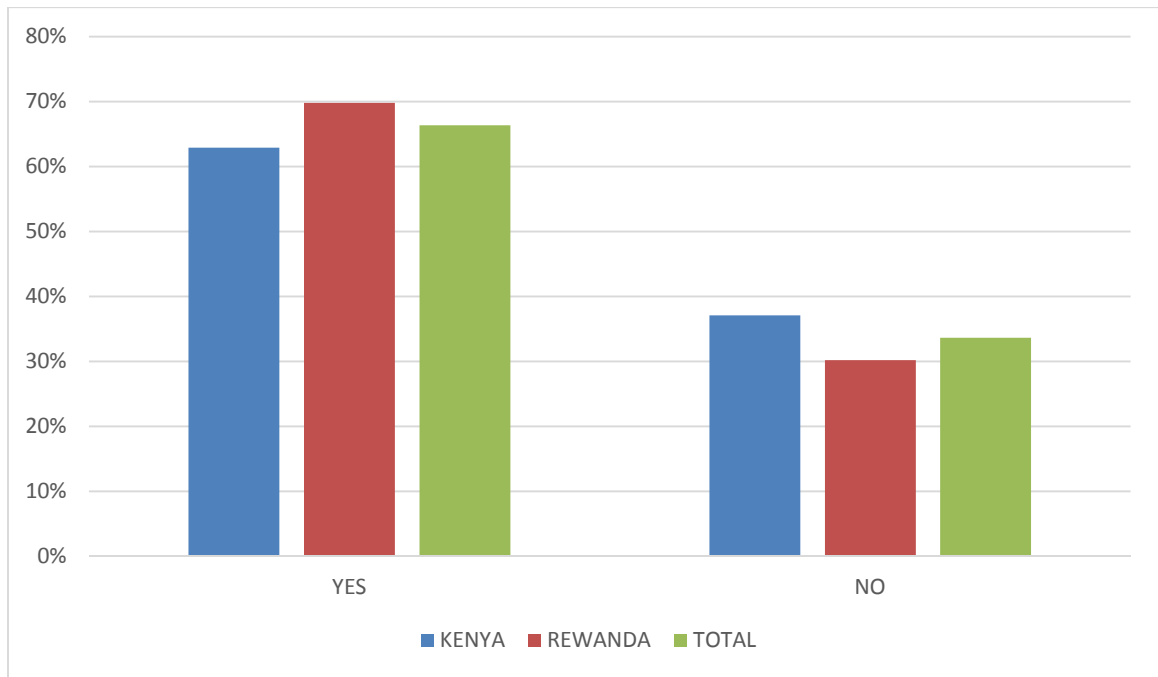


Figure 4.9: Legislations in countering cybercrime

The above graph depicts the respondents' views on whether there are sufficient laws in place to combat cybercrime. In Kenya, 62.9 percent of respondents stated there are appropriate laws in place to combat cybercrime, compared to 37.1 percent who said there are no laws in place. Rwanda's findings were similar; with 69.8% of respondents confirming that enough legislation exists, compared to 30.2 percent who claimed that no adequate legislation exists to combat cybercrime. When the results from the two countries are combined, 66.35 percent say there are appropriate laws in place to combat cybercrime, while 33.65 percent say there are none. Based on these findings, the study concluded that both countries investigated have enough legislation in place to combat cybercrime.

Table 4.3: Opinions on level of enforcement mechanisms

	KENYA	RWANDA	TOTAL
Very good	6.7%	24.6%	15.65%
Good	17.4%	48.2%	32.8%
Fair	47.2%	22.9%	35.05%
Poor	28.7%	4.3%	16.5%

The above table shows respondents' views on the effectiveness of enforcement tools in combating cybercrime. Rwanda performed highly, with 24.6 percent of respondents saying Rwanda has very good cybercrime mechanisms and 48.2 percent saying Rwanda has decent mechanisms, compared to 6.7 percent and 17.4 percent for Kenya. Kenya, on the other hand, received 47.2 percent of respondents who said it has fair enforcement methods and 28.7 percent who said it has weak enforcement mechanisms, compared to Rwanda's 22.9 percent and 4.3 percent.

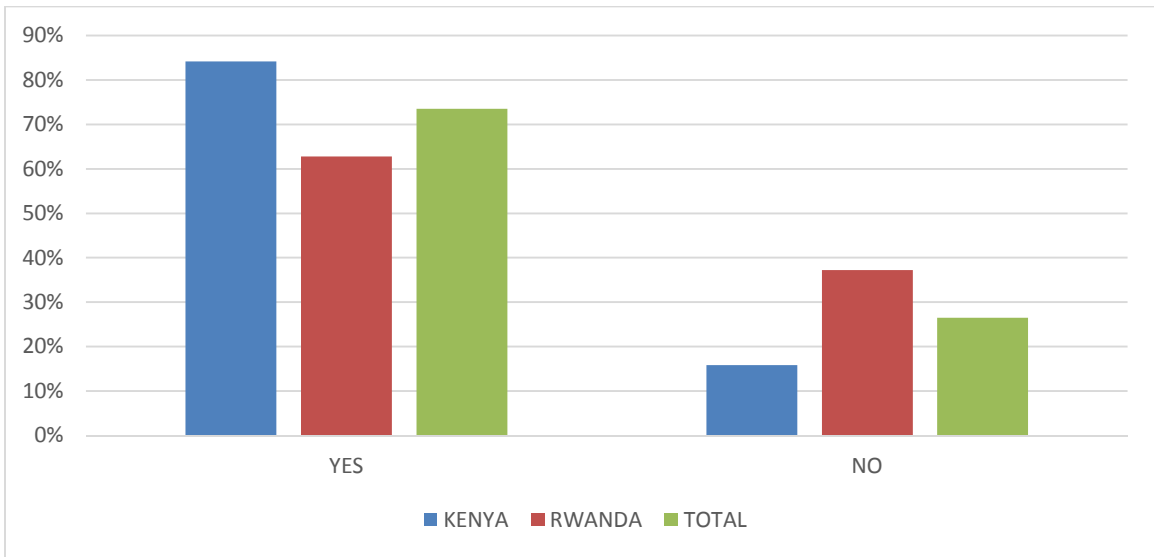


Figure 4.10: Difficult in identifying cybercrime criminals

The opinion of respondents on recognizing cybercrime criminals is depicted in the graph above. 73.5 percent of respondents in both countries agreed that identifying cybercrime perpetrators is difficult, while 26.5 percent stated it is not. The above table demonstrates how difficult it is to identify cybercrime criminals.

Table 4.4: Difficult in collecting cybercrime evidence

	KENYA	RWANDA	TOTAL
Very difficult	21.2%	17.7%	19.45%
Difficult	50.8%	48.5%	49.65%
Easy	19.1%	27.8%	23.45%
Very easy	8.9%	6%	7.45%

The above graph depicts the respondents' perspectives on the gathering of cybercrime evidence. It is widely acknowledged that gathering evidence to combat cybercrime is tough. In Kenya, 50.8 percent said it was challenging, and in Rwanda, 48.5 percent said it was difficult. Overall, 49.65 percent of respondents agreed that gathering evidence to combat cybercrime is challenging.

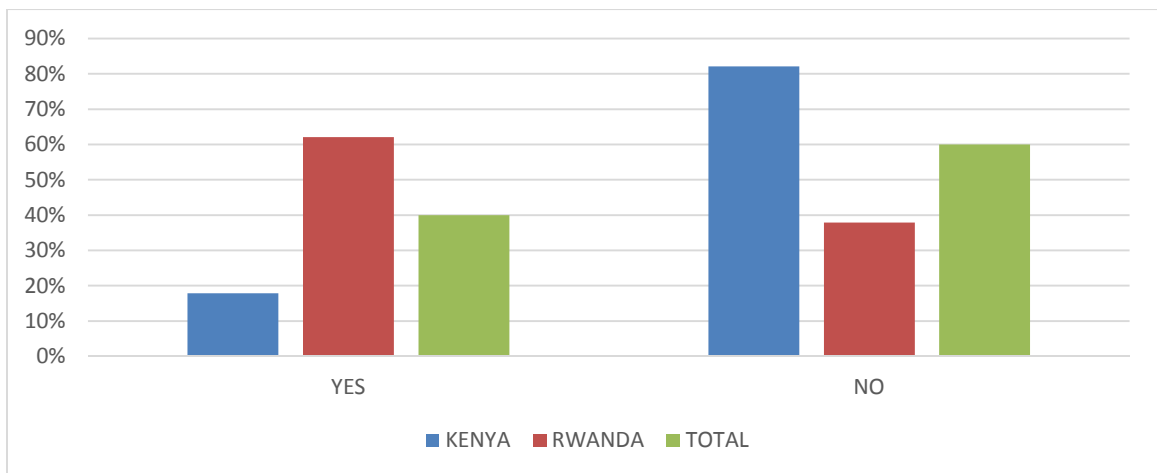


Figure 4.11: Training of law enforcers

The opinion of respondents on whether law enforcement officers were adequately trained is shown in Figure 4.11 above. In Kenya, 17.9% of respondents said law enforcement officers were adequately trained, compared to 82.1 percent who said officers were not adequately trained. In Rwanda, however, 62.1 percent of respondents thought that law enforcement officers were well taught, compared to 37.9% who said that law enforcement officers were not adequately trained. On average, the data suggest that 60% of respondents were not well trained, compared to 40% who felt law enforcement officers were properly taught. As a result, more law enforcement training is required.

Table 4.5: Remuneration of law enforcers

	KENYA	RWANDA	TOTAL
Yes	35.3%	67.4%	51.35%
No	64.7%	32.5%	48.65%

Respondents' views on law enforcement remuneration in the fight against cybercrime are depicted in the graph above. In Kenya, 35.3 percent of respondents felt law enforcement officers were well compensated, compared to 64.7 percent who believed law enforcement officers were underpaid to combat cybercrime. In Rwanda, however, the reaction was different: 67.4 percent of respondents thought law enforcement officers were adequately compensated, compared to 32.5 percent who said law enforcement officers were not sufficiently compensated to combat cybercrime. This demonstrates Rwanda's deliberate efforts to inspire cybercrime law enforcement officers.

Table 4.6: Cooperation between different countries

	KENYA	RWANDA	TOTAL
Not at all	11.7%	7.8%	9.75%
Less extent	29.3%	18.5%	23.9%
Moderately	54.6%	45.3%	49.95%
Large extent	4.4%	28.0%	16.2%
Very large extent	0%	0.4%	0.2%

The table above summarizes respondents' views on collaboration in the fight against cybercrime. In Kenya, 54.6 percent of respondents indicated there is moderate cooperation, compared to 0 percent who said there is extensive cooperation. In Rwanda, 45.3 percent of respondents said collaboration between countries was modest, while 0.4 percent said cooperation between countries was extensive. On average, 49.95 percent of respondents in the two countries said cooperation among different countries in combating cybercrime was moderate, compared to 0.2 percent who said cooperation among different countries was extensive. As a result, the overall level of cooperation among countries in combating cybercrime was moderate.

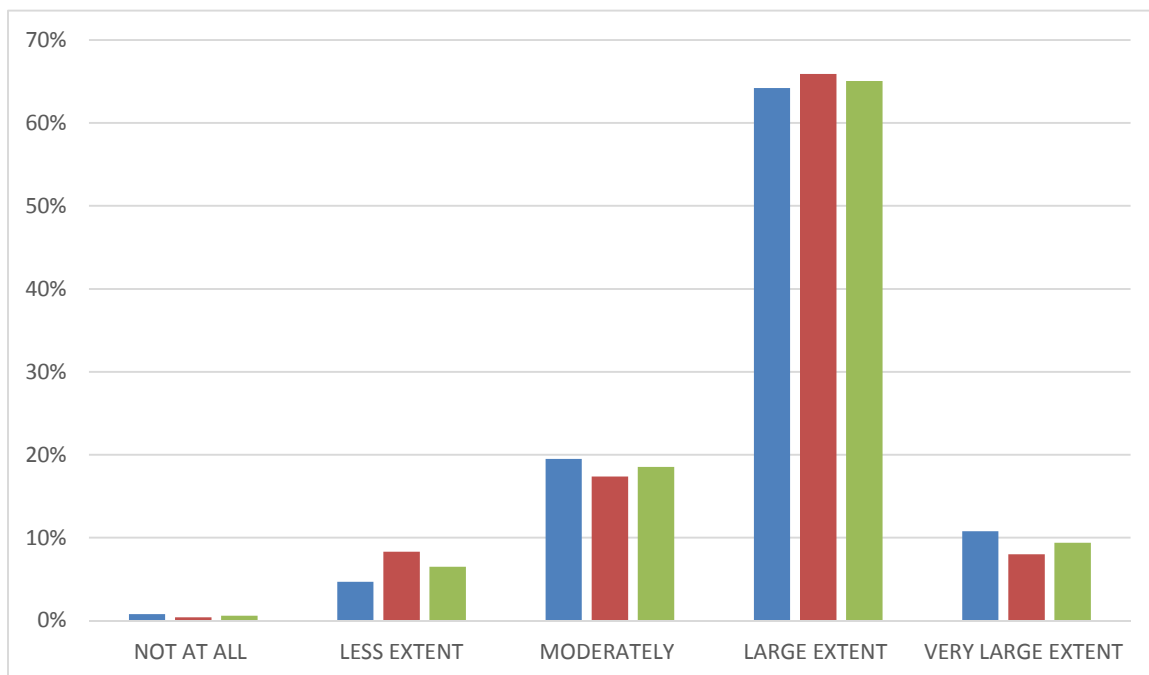


Figure 4.12: Current criminal laws and regulations coverage of cybercrime

Respondents' views on the extent to which present rules and regulations cover cybercrime are depicted in the graph above. The present criminal laws and regulations, in general, are thought to cover cybercrime to a great extent. In Kenya, for example, 64.2 percent of respondents agreed, while 65.9% of respondents in Rwanda agreed. On average, 65.05 percent of respondents believe that present anti-cybercrime rules and regulations effectively cover this area and that it is therefore not a major concern.

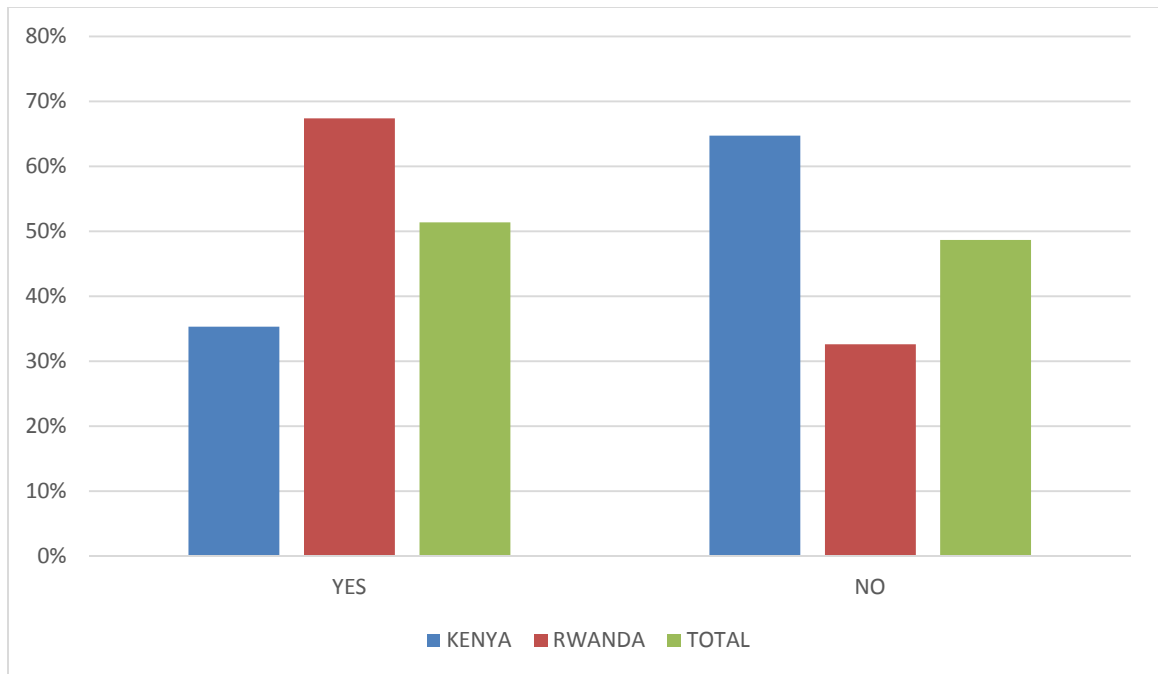


Figure 4.13: Enforcement of cybercrime laws and regulations

Respondents' views on whether cybercrime rules and regulations are sufficiently enforced are depicted in the graph above. In Kenya, 35.3 percent of respondents believed cybercrime laws were strictly enforced, compared to 64.7 percent who said cybercrime rules and regulations were not strictly enforced. In Rwanda, the contrary was confirmed: 68.2 percent of respondents believed cybercrime rules and regulations were well applied, whereas 31.8 percent felt they were poorly enforced. Rwanda has taken serious steps to implement cybercrime laws and regulations, as seen by this.

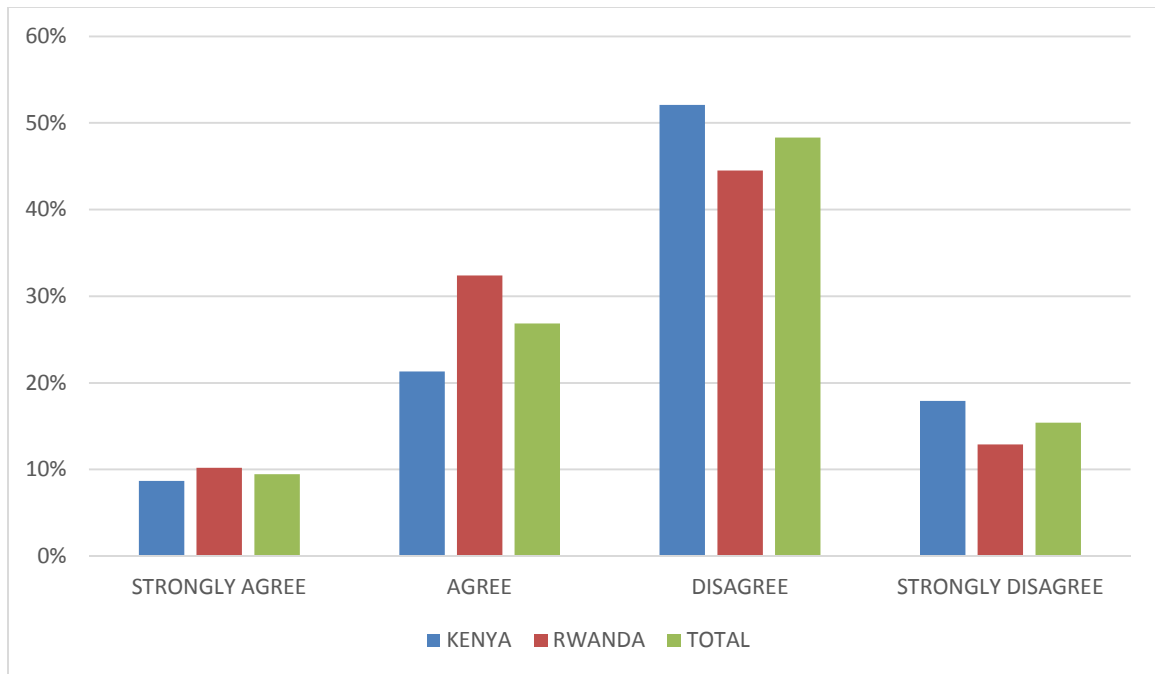


Figure 4.14: Uniformity of counter cybercrime laws

The graph above depicts respondents' views on the uniformity of anti-cybercrime legislation. In Kenya, 52.1 percent of respondents disagreed with the assertion that anti-cybercrime legislation is uniform in all nations, and 17.9 percent strongly disagreed. Only 8.7% of Kenyan respondents strongly agreed with the statement, while 21.3 percent simply agreed. In Rwanda, however, 44.5 percent disagreed with the assertion, with 12.9 percent strongly disagreeing. In Rwanda, 10.2 percent strongly agreed with the statement, while 32.4 percent agreed. In both nations studied, 48.3 percent disagreed while 15.4 percent strongly disagreed with the statement that counter-cybercrime legislation are uniform in all countries, compared to 26.85 percent who agreed and 9.45 percent who highly agreed. As a result, these findings reveal that anti-cybercrime legislation is not uniform in all countries.

Table 4.7: The effect of high speed of data exchange on cybercrime investigations

	KENYA	RWANDA	TOTAL
Strongly disagree	4.1%	6.9%	5.5%
Disagree	12.6%	9.8%	11.2%
Uncertain	8.2%	2.4%	5.3%
Agree	47.3%	48.8%	48.05%
Strongly agree	27.8%	32.1%	29.95%

The table above depicts how data exchange influences cybercrime investigations. According to Kenyan respondents, 47.3 percent agreed and 27.8 percent strongly agreed that the fast speed of data exchange processes has a detrimental impact on cybercrime investigations. In comparison, 12.6 percent disagree, with 4.1 percent strongly disagreeing. In Rwanda, the findings were similar, with 32.1 percent strongly agreeing and 48.8 percent agreeing that the fast speed of data transmission had an impact on cybercrime investigations compared to 6.9% who strongly disagreed and 9.8% who disagreed. The total results showed that 29.95 percent strongly agreed and 48.05 percent strongly disagreed, considerably outnumbering the 5.5 percent strongly disagreed and 11.2 percent disagreed. As a result, respondents from both nations in the study found that a high rate of data exchange has a detrimental impact on cybercrime investigations. One of the reasons offered is that, because cybercrime occurs through the use of computers and networks, much information changes on all systems with the push of a button, altering the meaning and outcomes of investigations. That a single easy action on one computer can wipe data from all other machines obstructing investigations.

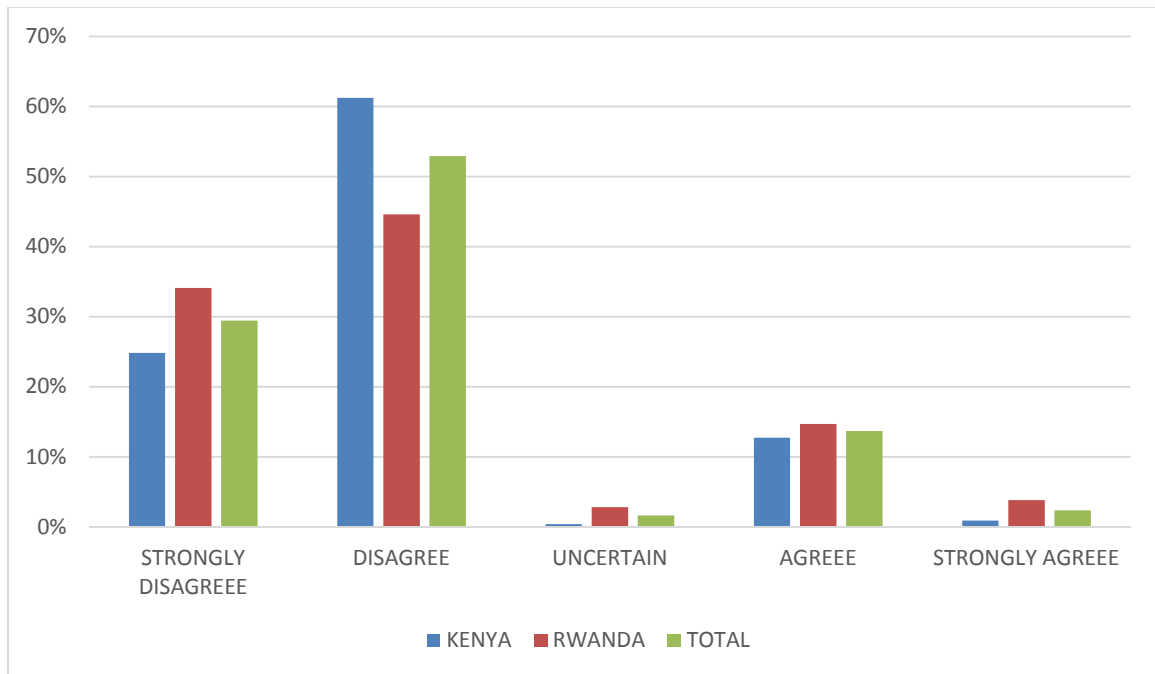


Figure 4.15: Opinions on total legal and international cooperation in countering cybercrime

The graph above depicts respondents' views on legal and global collaboration in the war against cybercrime. Kenyan respondents were divided on the assertion that there is complete legal and worldwide collaboration in the battle against cybercrime, with 24.8 percent strongly disagreeing and 61.2 percent merely disagreeing, compared to 0.9 percent highly agreeing and 12.7 percent simply agreeing. In Rwanda, however, 34.1 percent strongly disagreed, while 44.6 percent strongly disagreed, compared to 3.8 percent strongly agreed and 14.7 percent who concurred. Across total, 29.45 percent of respondents strongly opposed, while 52.9 percent strongly disagreed, compared to 2.35 percent who strongly agreed and 13.7 percent who agreed with the statement in the two countries studied. As a result of these findings, it can be concluded that there is no

comprehensive legal and international cooperation in the fight against cybercrime, making it one of the problems in the fight against cybercrime.

Table 4.8: Extradition as a challenge in countering cybercrime

	KENYA	RWANDA	TOTAL
Strongly disagree	3.1%	5.4%	4.25%
Disagree	10.2%	15.1%	12.6%
Uncertain	3.7%	2.1%	2.9%
Agree	54.3%	56.6%	55.45%
Strongly agree	28.7%	20.8%	24.75%

The table above depicts the responses to the statement that extradition is not a problem in the fight against cybercrime. In Kenya, 28.7% of respondents strongly agreed, and 54.3 percent agreed. 3.1 percent strongly disagreed and 10.2 percent disagreed, respectively. In Rwanda, 20.8 percent of respondents strongly agreed, while 56.6 percent strongly disagreed, with 5.4 percent strongly disagreeing and 15.1 percent disagreeing. In total, 24.75 percent of respondents strongly agreed, while 55.45 percent agreed with the aforesaid statement, compared to 4.25 percent who strongly disagreed and 12.65 percent who merely disagreed in both countries of study. The argument given was that countries cooperated bilaterally and multilaterally to find solutions to their problems as and when they arose.

Table 4.9: Readily available information on the internet as a challenge in counter cybercrime

	KENYA	RWANDA	TOTAL
Strongly disagree	3.8%	3.2%	3.5%
Disagree	18.7%	14.45	16.55%
Uncertain	4.2%	3.6%	3.9%
Agree	48.8%	52.6%	50.7%
Strongly agree	24.5%	26.2%	25.35%

Table 4.9 depicts respondents' views on the impact of publicly available information as a difficulty in the fight against cybercrime. The remark under consideration is that having access to easily available information on the internet is not a barrier to combating cybercrime. Respondents in Kenya and Rwanda agreed that having access to easily available information on the internet was not a significant issue in combating cybercrime. 25.5 percent strongly agreed, and 60.7 percent agreed, compared to 3.5 percent strongly disagreeing and 16.55 percent disagreeing.

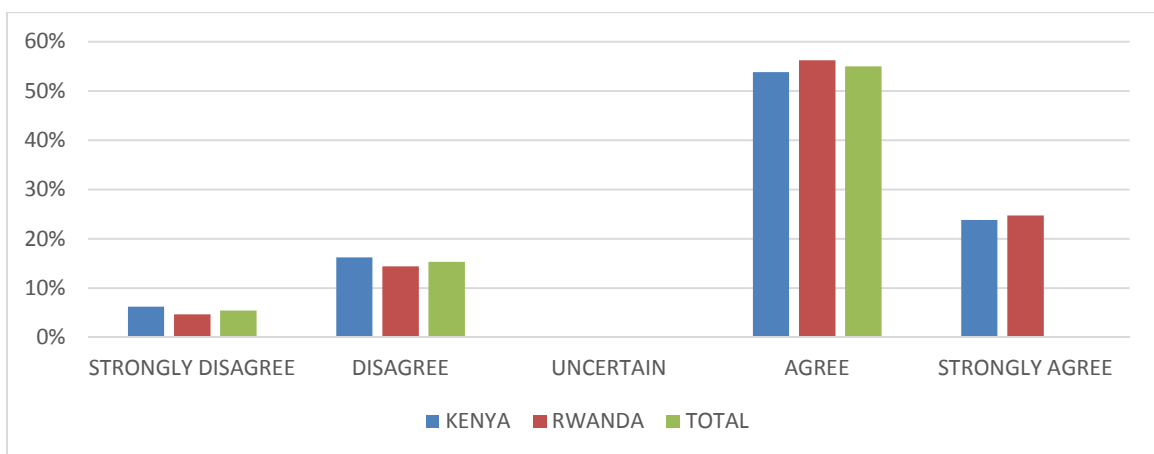


Figure 4.16: Covering o cybercrime by National criminal laws

The graph above depicts respondents' views on whether or not writing national criminal legislation adequately covers cybercrime. In Kenya, 23.8 percent of respondents strongly agree, while 53.8 percent agree, with 6.2 percent strongly disagreeing and 16.2 percent disagreeing. In Rwanda, 24.7 percent of respondents strongly agreed, while 56.2 percent agreed, with 4.75 percent strongly disagreeing and 14.4% merely disagreeing. Both countries had a result of 24.25 percent highly agreeing and 55.0 percent agreeing, compared to 5/45 percent strongly disagreeing and 15.3 percent disagreeing. This indicates that a higher number of respondents in both nations of study confirmed that cybercrime is covered when writing national criminal legislation.

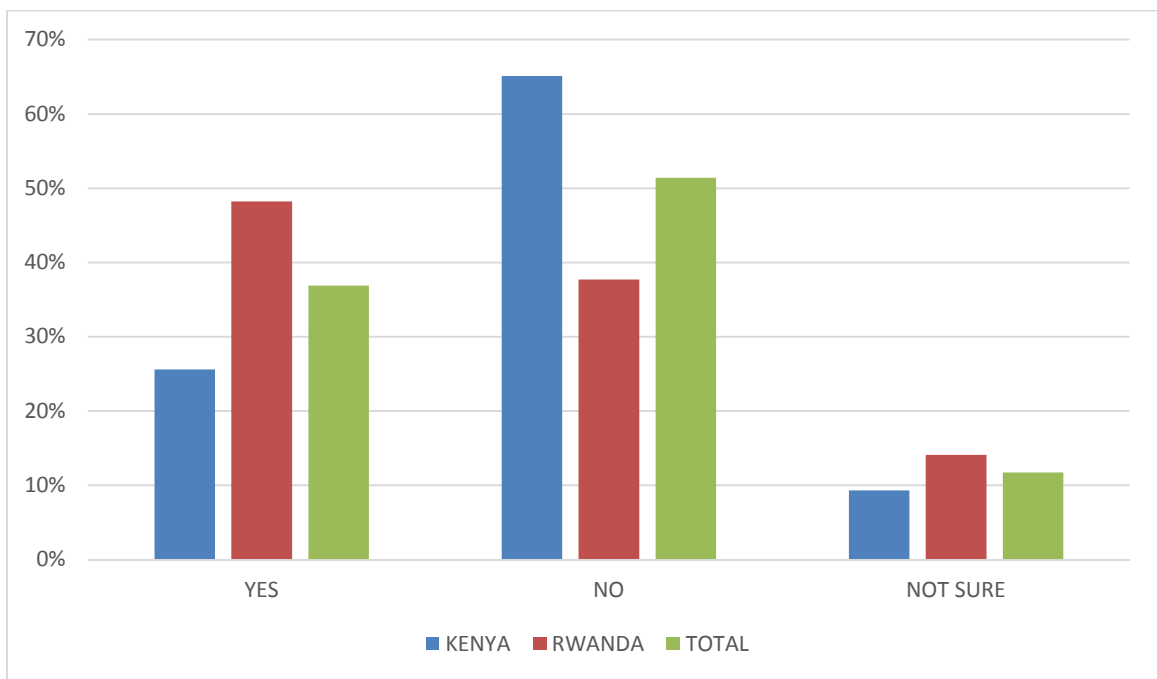


Figure 4.17: Mechanisms of monitoring and regulating the internet

Figure 4.17 depicts respondents' views on procedures for monitoring and regulating the internet in both research nations. In Kenya, 65.1 percent of respondents stated there are no measures in place to monitor and regulate the internet, while only 25.6 percent claimed

there are. In Rwanda, however, 37.7% of respondents said there are no processes in place, compared to 48.2% who said there are mechanisms in place. When comparing the two study countries, it goes without saying that Rwanda has more procedures in place than Kenya. As a result, Kenya may learn from Rwanda about how they ensure that processes, as well as monitoring and regulation, are in place.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary, Conclusion and Recommendations

This chapter provides a summary of the entire study, highlighting the paper's significant contributions and accomplishments, as well as possible recommendations for policymakers and practitioners to improve the way they combat cybercrime. The objectives were re-stated, and the data gathered was presented, analysed, and analysed to help the researcher make an informed decision about the counter-cybercrime difficulties facing twenty-first-century Africa, with an emphasis on Kenya and Rwanda. It also identifies potential study directions for related studies.

5.2 Summary of the Study

The goal of this research was to better understand the issues of counter-cybercrime in twenty-first-century Africa, particularly in Kenya, in order to develop potential solutions. The study was prompted by the growing issues of counter-cybercrime in Kenya, as well as the necessity to propose potential solutions for dealing with the situation. The study also wanted to know why, despite the fact that there are measures in place to combat cybercrime, there are still problems. The researcher evaluated literature directed by the established objectives to gain a better understanding of the issues of counter-cybercrime in twenty-first-century Africa, particularly in Kenya and Rwanda; the updated literature identified the study's existing deficiencies. Furthermore, both qualitative and quantitative approaches were used by the researcher to obtain responses to the study's questions. The

major goal of this study was to see how the obstacles of combating cybercrime have hampered diverse tactics internationally, regionally, and nationally.

The goal of the study was to look at the many obstacles that different jurisdictions throughout the world have in combating cybercrime, as well as their tactics to overcoming those challenges in order to effectively combat cybercrime.

This research looked at the methods used to combat cybercrime around the world, as well as in Africa, Rwanda, and Kenya. In the example of Rwanda, the research looked at the elements that helped it outperform Kenya in the fight against cybercrime.

Rwanda was also chosen because it has done a good job combating cybercrime, and is now the best in East Africa. Kenya may learn from Rwanda's initiatives, regulations, and management strategies. Rwanda is likewise a fast-developing economy in East Africa, making her a suitable model to follow. Kenya is included because the paper was created in Kenya with the goal of determining the best strategies to combat cybercrime concerns that may be implemented by the Kenyan government.

5.3 Summary of the Findings

Four objectives were re-examined in summarizing the findings of this study:

- (i) Assessing the worldwide difficulties of counter-cybercrime
- (ii) Critical examination of the challenges of counter-cybercrime activities in Africa

(iii) To analyse and contrast the problems confronting Kenya's and Rwanda's counter-cybercrime efforts.

(iv) Provide applicable policies and methods for addressing counter-cybercrime concerns in Kenya.

In terms of the first goal, members of the European legal community regularly cited the complexity of cybercrime cases from a jurisdictional standpoint as one of the major problems. The fundamental premise of a territorially oriented investigative strategy conflicted with the international nature of cybercrime, according to the 2014 Internet Organized Crime Threat Assessment (IOCTA) report. One of the most frequently noted issues by cybercrime law enforcement officers is the capacity to quickly collect data and information beyond traditional jurisdictional boundaries, in addition to the cross-border characteristics of cybercrime.

In terms of the second goal, new sorts of crime were discovered to have emerged, and traditional crimes such as fraud were now being perpetrated using sophisticated methods as a result of the emergence of new technologies. While traditional boundaries have melted away, the platform for committing crime has now become a virtual borderless globe. Because no physical presence between a victim and a perpetrator is required, cybercrime defies the issue of jurisdiction, further complicating the difficulty of detection. Due to the additional resources required to track down cyber criminals in multiple nations, as well as jurisdictional issues, there are few trials of offenders breaking cyberspace laws.

Cybercrime Legislation is the other challenge that African countries face, according to this study. Cybercrimes are committed in an electronic medium that defies the laws that govern traditional crimes conducted in a physical medium.¹⁰⁹

In many cases, regulations pertaining to physical crimes are insufficient to handle crimes committed using automated means. The legal systems of African countries were founded on the vestiges of colonial laws. Because they were colonized by the British, countries like Nigeria, Kenya, and Uganda had their laws based on British common law. Others, such as Ivory Coast, Gabon, and the Democratic Republic of Congo, were governed by French civil law because they were colonized by the French. The situation was more problematic for countries like Cameroon, which had both British and French colonial overlords. These countries were compelled to work with both British and French Civil and Common Laws at the same time, which proved to be a difficult task. As a result of the legislative inconsistencies, many African states tackled cybercrime differently, resulting in a lack of harmonization. Collaboration in resolving crime and prosecuting perpetrators becomes a major challenge when one country's laws forbid specific behaviors but another country's laws do not do so to the same extent.

The lack of harmonized rules and regulations, low capacity building for investigators, insufficient resource allocation, and poor remuneration of counter cybercrime officers are all shared difficulties in both Kenya and Rwanda, according to objective three. Both

¹⁰⁹M. Watney The Evolution of legal regulation of the Internet to address terrorism and other crimes' (2007) 3 *Tydskrif vir die Suid- Afrikaanse Reg* 469

countries face the problem of a lack of legal and international collaboration in the fight against cybercrime. In comparison to Kenya, however, this study found that Rwanda is doing a better job of enforcing cybercrime laws and regulations. In comparison to Kenya, Rwanda has prioritized law enforcement training. Rwanda is also doing well in terms of remunerating law enforcement officers and allocating resources strategically to combat cybercrime.

The fourth goal is to provide appropriate policies and tactics for dealing with Kenya's counter-cybercrime concerns. This has been well conveyed in the study's recommendation.

5.4 Conclusions

According to the literature studied, there is widespread international agreement that additional efforts should be made to improve the skills needed to cope with the cybercrime threat to governments and organizations. There is no single international legislation binding states to work together to combat cybercrime. Because of the issues of sovereignty and jurisdiction among countries, it is difficult for individual governments to investigate and successfully prosecute cybercrime. There are also good rules and legislation, but implementation is the issue. In Kenya, for example, there were already laws in place to deal with cybercrime before to 2018, but instead of putting them into effect, the government enacted the Computer and Cybercrimes Act, which was met with skepticism by lawyers and other cybercrime stakeholders.

There are various obstacles to overcome, including absence of capability and technical difficulties in developing an operable criminal justice response to cybercrime. Gaps in legal enactment skills in different countries are a major source of concern, as they obstruct international investigations. A lack of powerful and harmonized legal apparatuses across jurisdictions, as well as ensuring that law enforcement has sufficient skills and knowledge to effectively investigate and prosecute cybercrime, is another obstacle. There is also a need for more effective access to and ability to use electronic evidence, as well as the application of scientific talents. The role of the business sector in addressing cybercrime and coordinating efforts, notably in Kenya, requires more attention. There is minimal effort in the field of combating computer crimes in terms of research and development, making it difficult for Kenya to come up with innovative and effective approaches to tackle cybercrime. The training and remuneration of law enforcement officers involved in counter-cybercrime is insufficient. As a result, the officers involved lack the necessary skills, expertise, and morale to combat cybercrime.

Because Kenyan efforts to prevent Internet crime are still dominated by aggressive and response legislation, it is critical to restructure the existing criminal code to address offenses such as unauthorized entry, fraud, child pornography, and copyright infringement. However, a logical approach to combating cybercrime is still in its infancy. Some sophisticated criminals have turned to cybercrime to collect assets or disrupt corporations or organizations on a global, regional, and national scale. Technology has advantages and disadvantages depending on the user's goal. Computer crime, commonly known as cybercrime, is rapidly becoming one of the most serious threats to the worldwide

well-being of nations. To effectively deal with such illegal conduct, there is a critical need for a common understanding of it on a global scale. It is also critical to thoroughly investigate and analyze the problem, as well as to identify roadblocks to global collaboration in the fight against cybercrime.

5.5 Recommendations

The issues revealed in this study confirm that they are roadblocks to addressing Kenya's cybercrime problem. It brings the difficulties that different countries confront in combating cybercrime into sharper focus, allowing for a better appreciation and understanding of the issues.

The first recommendation made by this study is the necessity to establish a universally recognized law that will apply throughout the world, thereby making the entire world one jurisdiction. Regardless of where a cybercrime is committed, the perpetrator can be apprehended. Kenya should band together with other like-minded nations to press for the implementation of this international law. Meanwhile, Kenya should establish as many bilateral and multilateral cooperation agreements as feasible in the area of extradition of all criminals (Cyber criminals included).

As this study and previous studies have shown, cybercrime impedes a nation's growth and development by causing insecurity and instability. In order to deal with the various hazards posed by cybercriminals, this report recommends that Parliament pass more rigorous and punishing regulations in comparison to the current computer cybercrime

laws. Before the proposed law is passed, the Kenya Information Communication Act, the Penal Code, and its recommendations, which already punish cybercrime, should be implemented and vigorously enforced.

The different bodies and instruments must work together to ensure that the ensuing cybercrime policy and legislative environment is supportive of human rights-based approaches to cyber security.

When it comes to national security issues, cybercrime should be at the forefront. Staff training and capacity building should be established and implemented on a continuous basis to increase their knowledge and abilities, allowing them to stay ahead of cyber criminals and keep up with current cybercrime trends and the dynamic nature of cybercrime. Furthermore, cease making political appointments in the field of cyber security and instead hire the proper people who meet the necessary qualifications, since security is vital.

A national education and awareness campaign on the importance and impact of cyber security is critical in lowering the country's cybercrime rate. It is critical to raise information security awareness and skills, as well as share best practices, through cyber security culturization at all stages.

Since cybercrime affects many sectors of the economy, a multi-sector solution to cybercrime concerns should be required. In addition, when dealing with cybercrime situations, state security authorities should be watchful and proactive.

Cyber-related offenses should be investigated and prosecuted by a special unit within the Directorate of Criminal Investigation (DCI) and the Armed Forces. The same unit should be well-equipped to carry out its responsibilities. To deal with this sophisticated and dynamic crime, digital processing should be enhanced, and a contemporary digital forensic laboratory should be built. The proposed contemporary forensic facilities will save time processing the essential evidence, allowing investigators and prosecutors to spend less time on the case. To investigate all cybercrime-related offences across the country, forensic laboratories should be established. This will serve as a deterrent to cybercriminals who are roaming the country committing crimes.

In order to record all citizens' biometric data and other critical details that should be cross-matched in the event of a crime, a national database system should be designed and deployed. As a result, the problem of anonymity will be solved because all records will be available for cross-checking.

5.6 Suggestions for Further Research

A study should be performed to address the need for internationally harmonized cybercrime laws and regulations, as well as international collaboration in the fight against cybercrime.

BIBLIOGRAPHY

Books

- Akers, Ronald L. and Christine Sharon Sellers, 2009, *Criminological theories: introduction, evaluation, and application*. New York: Oxford University Press.
- Brenner S. W., 2010, *Cybercrime, Criminal Threats from Cyberspace*, Santa Barbara, California
- Clough, J. 2015, *Principles of cybercrime*, Second edition, Cambridge University Press
- Gercke, M. 2012 “Cybercrime”, *Understanding Cybercrime Phenomena, Challenges and legal response*, September 2012
- Kirwan, D (2017), *An Investigation of the Attitudes and Environmental factors that make people more willing to participate in online crimes*, Masters Dissertation, Dublin Institute of Technology
- Mugenda O. and Mugenda A, 2003, *Research Methods, Qualitative and Quantitative Approaches*, Acts Press, Nairobi- Kenya
- Nachmias, C. and Nachmias, D. 1985, *Research Methods in Social Sciences*. London: Edward Anold,
- Newburn, T., (2008), *Handbook of Policing*, 2nd ed. William publishing, Devon
- Nir Kshetri, 2006, *the Simple Economics of Cybercrime*, University of Carolina, U S A
- Poonia, A. S. 2014, *Cyber Crime: Challenges and its Classification*, *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, ISSN, 2278-6856.
- Schelling, T. C. 1980, *The strategy of conflict: [with a new preface]*. Cambridge, Mass: Harvard Univ. Press.
- Souter, David and Monica Kerretts-Makau, 2012. *Internet Governance in Kenya-An Assessment for the Internet Society* <http://www.internetsociety.org/sites/default/files/ISOC>
- Stavrou A. 2001, *Mission Impossible: E- security in South Africa’s Commercial and Financial Sectors*, Institute for Security Studies, Pretoria

Journals

Adoption of Convention on Cybercrime, *The American Journal of International Law*, Vol. 95, No. 4 (Oct., 2001), pp. 889-891 Published by: Cambridge University Press Stable URL: <https://www.jstor.org/stable/2674643> Accessed: 23-01-2020 19:18 UT

Ajayi, E. F. G. Challenges to enforcement of cyber-crimes laws and policy, *Journal of Internet and Information Systems*, School of Law, Kenyatta University, Nairobi, Kenya. 25 July, 2016

Brenner and Bert-Jaap Koops, 'Approaches to cybercrime jurisdiction' (2004) *Journal of High Technology Law*

Cameron S. D. Brown, *International Journal of Cyber Criminology* Vol. 9 Issue 1 January – June 2015 Australian National University, Australia

Casey, *Digital Evidence and Computer Crime*, 2004, page 11; Lange/Nimsger, *Electronic Evidence and Discovery*, 2004, 1; Hosmer, *Proving the Integrity of Digital Evidence with Time*, *International Journal of Digital Evidence*, 2002, Vol.1, No.1,

Casey, *Error, Uncertainty, and Loss in Digital Evidence*, *International Journal of Digital Evidence*, 2002, Vol. 1, Issue 2.

Cybercrime theory and discerning if there is a crime: the case of digital piracy Author(s): Frances P Bernat and David Makin Source: *International Review of Modern Sociology*, Vol. 40, No. 2 (Autumn 2014), pp. 991-19 Published by: International Journals Stable URL: <https://www.jstor.org/stable/43499904> Accessed: 18-01-2020 09:44 UTC

Fawzia Cassim, *Addressing the growing spectra of cybercrime in Africa: Evaluating Measures Adopted by South Africa and other regional role players*, *The Comparative and International Law Journal of Southern Africa*, Vol. 44, No. 1 (MARCH 2011), pp. 123-138 Published by: Goodman, M., *why the Police don't care about cybercrime*, *Harvard Journal of law and technology* (10) (1997)

Global Fight Against Cybercrime: Undoing the Paralysis Author(s): Zahid Jamil Source: *Georgetown Journal of International Affairs*, *International Engagement on Cyber 2012: Establishing Norms and Improving Security* (2012), pp. 109-120 Published by: Georgetown University Press Stable URL: <https://www.jstor.org/stable/43134344> Accessed: 20-01-2020 15:19 UTC

Goodman & S Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' 2002 *International Journal of Law and Information Technology* 139-223 at 142, 146-150.

- Guha Digijah, Cybercrimes, Challenges and Solutions, International Journal of Computer Science and Information Technologies, volume 4, September 2013
Journal of International Affairs, Vol. 66, No. 1, Transnational Organized Crime (Fall/Winter 2012), pp. vii-ix Published by: Journal of International Affairs Editorial Board Stable URL: <https://www.jstor.org/stable/24388246> Accessed: 26-01-2020 12:13 UTC
- Karuppana Jaishankar, Space Transition Theory of Cybercrime, International Journal of Cyber Criminology Vol1 Issue 2 July 2007
- Keyser, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289,
- Liff, A. P. (2012). Cyber war: A new “absolute weapon”? The proliferation of cyber warfare capabilities and interstate war. *Journal of Strategic Studies*, 35(3), 401-428. <https://doi.org/10.1080/01402390.2012.663252>
- Longe, O and Chiemekwe, S. Cybercrime and criminality in Nigeria – What roles is internet access points in playing? *Eur. Journal. Soc. Science*. 6(2008):133-139.
- Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004,
Mike Keyser, ‘Council of Europe Convention on Cybercrime’ (2002) *J. Transnational & Policy* 12, 287.
- Moore, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, *American Journal of Criminal Justice*, Vol. 29, No. 1, 2004,
- Mr. SC Ahmet Nuredini, PhD Candidate Professor in ISPE College, Challenges in Combating the Cybercrime, *Mediterranean Journal of Social Sciences*, Vol. 5 No 19 August 2014, MCSER Publishing, Rome-Italy
- Nir Kshetri (2019) Cybercrime and Cyber security in Africa, *Journal of Global Information Technology Management*, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527
- Renner 'Cybercrime investigation and prosecution: the role of penal and procedural law' 2001 Murdoch University Electronic Journal of Law
- Ryan, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging
Salil K. Mehra, Law and Cybercrime in the United States Today, *The American Journal of Comparative Law*, Vol. 58, Supplement: Welcoming the World: U. S. National Reports to the XVIIIth International Congress of Comparative Law (2010), pp. 659-685 Published by: Oxford University Press.
- Satya Deva Bedi, ‘Extradition in international law and practice’ (Rotterdam, 1966) 69;
Bassiouni M. Cherif, “Political Offense Exception Revisited: Extradition between

the US and the UK-A Choice between Friendly Cooperation among Allies and Sound Law and Policy” (1986) *The Denv J/Int'l L & Ploy*, 15, 255.

Snail S ‘Cybercrime in South Africa Hacking, Cracking and Other Unlawful Online Acts’ (2009) *Journal of information, law and technology*

Sussmann, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, *Duke Journal of Comparative & International Law*, 1999, Vol. 9, page 451

The Council of Europe's Convention on Cybercrime Author(s): Amalie M. Weber Source: *Berkeley Technology Law Journal*, Vol. 18, No. 1, Annual Review of Law and Technology (2003), pp. 425-446 Published by: University of California, Berkeley, School of Law Stable URL: <https://www.jstor.org/stable/24120528> Accessed: 18-01-2020 09:07 UTC

Other references

“The Wireless Internet Opportunity for Developing Countries”, 2003, available at: 2006 E-Crime Watch Survey, page 1, available at: www.cert.org/archive/pdf/ecrimesurvey06.pdf.

Act No 4 of 2000, Laws of Kenya.

Agwe Eric, et al, *Combating Cybercrime in Sub Sahara Africa; A Discourse on Law, Policy and Practice*, Nelson Mandela School of Public Policy, Southern University Baton Rouge, Criminal Justice Department, Southern University Rouge, January 2011.

Alkaabi Ali O S, 2010, *Combating Computer Crime: An International Perspective*, Thesis Submitted in accordance with the regulations for Degree of Doctor of Philosophy, University of Southern Queensland.

Allison Peters and Amy Jordan, *Countering the Cyber Enforcement Gap, Strengthening Global Capacity on Cybercrime, Third Way* (2019) Stable URL: <https://www.jstor.org/stable/resrep20150> Accessed: 15-02-2020 06:13

Baker, Al. “An ‘Iceberg’ of Unseen Crimes: Many Cyber Offenses Go Unreported.” *The New York Times*, the New York Times, 5 Feb.

Bellovin and others, *Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP*, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf;

Bellovin et al, *Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP; Simon/Slay, Voice over IP: Forensic Computing Implications*, 2006;

- Chibuko Raphael Ibekwe, Thesis submitted to School of Law, University of Stirling the Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions, July 2015
- Common challenges in combating cybercrime as identified by Euro just and Europol June 2019, Joint Report, Europol and Euro just Public Information Communications).
- Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, Vienna, 25-28 February 2013
- Countering the Cyber Threat Author(s): Shawn Henry and Aaron F. Brantly Source: The Cyber Defense Review, Vol. 3, No. 1 (SPRING 2018), pp. 47-56 Published by: Army Cyber Institute Stable URL: <https://www.jstor.org/stable/10.2307/26427375>
- Cybercrime and Intellectual Property section of the National Informational Infrastructure Protection Act of 1996: Legislative analysis (U.S. Department of Justice)
- Cybercrime and Intellectual Property section of the National Informational Infrastructure Protection Act of 1996: Legislative analysis (U.S. Department of Justice)
- Cybercrime and Intellectual Property section of the National Informational Infrastructure Protection Act of 1996: Legislative analysis (U.S. Department of Justice) Dr. Russell G. Smith, Investigating Cyber Crime: Barriers and Solution, Pacific Rim Fraud Conference, 2003
- Cybercrime and Intellectual Property section of the National Informational Infrastructure Protection Act of 1996: Legislative analysis (U.S. Department of Justice)
- Cynthia E Jones, 'Evidence destroyed, innocence lost: The preservation of biological evidence under innocence protection statutes' (2005) Am Crim L Rev 42,
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic
- Dr. Julien Jeandesboz et al, The Law Enforcement Challenges of Cybercrime: Are we really playing catch-up? Study of the LIBE Committee, 2015
- Dr. Russell G. Smith, Investigating Cyber Crime: Barriers and Solution, Pacific Rim Fraud Conference, 2003
- Erin Murphy, 'the new forensics: Criminal justice, false certainty, and the second generation of scientific evidence' (2007) California Law Review 721-797;

- Erin Murphy, 'The new forensics: Criminal justice, false certainty, and the second generation of scientific evidence' (2007) *California Law Review* 721-797; Cynthia E Jones, 'Evidence destroyed, innocence lost: The preservation of biological evidence under innocence protection statutes' (2005) *Am Crim L Rev* 42,
- Fachkha, C., & Debbabi, M. 2016, Dark net as a source of cyber intelligence: Survey, taxonomy, and characterization. *IEEE Communications Surveys & Tutorials*, 18(2), 1197-1227. <https://doi.org/10.1109/COMST.2015.2497690>
- Filing Complaint with the Internet Crime Complaint Centre (IC3), Federal Bureau of Investigation, and www.ic3.gov/.
- G. Gordon 'The hidden economy of cyber-crime' *Sunday times* 12 February 2012.
- Gabuardi, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, *Mexican Law Review*, Vol. I, No. 2, page 156,
- George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, and Alan Schwartz, 'Information Technology Security Handbook' (Washington, DC: World Bank, 2003)
- Gercke, Use of Traffic Data to trace Cybercrime offenders, DUD 2002
- Global Economic Survey 2018 (Rwanda Report)
- Goerling, The Myth of User Education, 2006 at www.parasiteconomy.com/texts/StefanGorlingVB2006.pdf.
- Gordon G. 'The hidden economy of cyber-crime' *Sunday times* 12 February 2012.
- Government of Rwanda (2000), An Integrated ICT-led Socio – Economic Development Plan for Rwanda 2000-2010
- Graycar, A. (2001, June 21-22). New crimes or new responses. Speech presented at 4th National Outlook Symposium on Crime in Australia: New Crimes or New Responses. Canberra: Rydges Lakeside.
- Her majesty's Inspectorate of Constabulary. Inspection Report Metropolitan Police, October 2007 <http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm>.
- Ian Volek, "Federal Rule of Evidence 703: The Back Door and the Confrontation Clause, Ten Years Later" (2011) *Fordham l REV*, 80, 959,
- Institute for Security Studies, The AU's Cybercrime report, A Positive Start, but Substantial Challenges Ahead

- Institute of Foreign and Comparative Law Stable URL:
<https://www.jstor.org/stable/23253117> Accessed: 20-01-2020 15:43 UTC
- International Telecommunication Union ITU Toolkit for Cybercrime Legislation. 2009
 Updated in February 2010, available from: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf>
- Ishan Mehta, The Need for Better Metrics on Cybercrime, Third Way (2019) Stable URL:
<https://www.jstor.org/stable/resrep20149> Accessed: 14-03-2020 07:47 UTC
- Jackson/Grunsch/Claypoole/Lamont, Blind Steganography Detection Using a
 Computational Immune: A Work in Progress, International Journal of Digital
 Evidence, available at: [www.utica.edu/academic/institutes/ecii/
 publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf](http://www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf);
- Jobel Kyle, Vecinon United by Necessity, The Cyber Defense Review, special edition:
 International Conference on Cyber Conflict (CYCON U.S.), November 14-15,
 2018: Cyber Conflict during Competition (2019), pp. 123-144 Published by: Army
 Cyber Institute Stable URL: <https://www.jstor.org/stable/10.2307/26846124>
- Kahn, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58,
- Keizer, Dutch Botnet Suspects Ran 1.5 Million Machines, TechWeb, 21.10.2005,
 available at: Kenya Gazette Supplement Acts, 2018, the Computer Misuse and
 Cybercrimes Act, No. 5 of 2018
- Kirwan Dearbhail, Cybercrime: An Investigation of the Attitudes and Environmental
 Cybercrime: An Investigation of the Attitudes and Environmental Factors that
 Make People more Willing to Participate in Online Crime, Technological
 University Dublin, Dissertations2017-9, School of Computing
- Law society of Kenya versus the Attorney general of Kenya and four others, LSK
 Challenges Constitutionality of the Computer Misuse and Cybercrimes Act, June
 2018
- Legal Brief E Law & Management Cyber law & Technology Watch Issue No: 1581 29th
 2015
- Lilly Pijnenburg Muller, 'Cyber Security Capacity Building in Developing Countries:
 Challenges and Opportunities' (2015)
- Lowman, The Effect of File and Disk Encryption on Computer Forensics, 2010,
 available at: [http://lowmanio.co.uk/share/The%20Effect%20of%20File%
 20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf](http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf).

- Luigino Bruni & Pier Luigi Porta (2014) Cesare Beccaria's On Crimes and Punishments, *History of Economics Review*, 60:1, 64-74, DOI: 10.1080/18386318.2014.11681265 <https://doi.org/10.1080/18386318.2014.11681265>
- M Sulfab 'Challenges of cybercrime in South Africa', research paper for Master of Arts in national security studies, American Military University (2014)
- Maat S., *Cybercrime: A Comparative Law Analysis*', Unpublished, LL M dissertation, University of South Africa (2009)3.
- Magutu Peterson, *Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment In Kenya*, University of Nairobi, 2011
- Mark Galeotti, *The cyber menace*, *The World Today*, Vol. 68, No. 7 (December 2012 & January 2013), pp. 32-35 Published by: Royal Institute of International Affairs Stable URL: <https://www.jstor.org/stable/41962876> Accessed: 24-01-2020 18:43 UTC
- Mike Keyser, 'Council of Europe Convention on Cybercrime' (2002) *J. Transnational & Policy* 12, 287.
- Ministry of Information Communication and Technology, *National Cyber security Strategy report*, 2014
- Mugisha, David, *Annual INTERPA Conference, Methods to Combat Cybercrimes in Rwanda*, 2019
- Nanjira Sambuli, etal, *Global Partners Digital, Mapping the Cyber Policy Land Scape: Kenya*, November 2016
- Ndayisabye H, 2011, *Cybercrimes in Rwanda, an Investigative case study of pirating in Nyarungenge District, 2005-2010*
- Nir Kshetri, *Diffusion and Effects of Cyber-Crime in Developing Economies*, *Third World Quarterly*, Vol. 31, No. 7 (2010), pp. 1057-1079 Published by: Taylor & Francis, Ltd. Stable URL: <https://www.jstor.org/stable/27896600> Accessed: 20-01-2020 15:47 UTC
- Oxford Dictionary of Law, 2002
- Peisert, S etal, 2014, *Designed-in Security for Cyber-Physical Systems*. *Security & Privacy*, IEEE, 12(5), 9-12.
- Rwanda: 2016 law governing information and communication Technologies, *Legal analysis*, may 2018

- Satya Deva Bedi, 'Extradition in international law and practice' (Rotterdam, 1966) 69; Bassiouni M. Cherif, "Political Offense Exception Revisited: Extradition between the US and the UK-A Choice between Friendly Cooperation among Allies and Sound Law and Policy" (1986) *The Denv J/Int'l L & Ploy*, 15, 255.
- Shawn Henry and Aaron F. Brantly, Countering the Cyber Threat, *The Cyber Defense Review*, Vol. 3, No. 1 (SPRING 2018), pp. 47-56 Published by: Army Cyber Institute Stable URL: <https://www.jstor.org/stable/10.2307/26427375>
- Simon/Slay, Voice over IP: Forensic Computing Implications, 2006, available at http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.
- Staniford /Paxson/Weaver, How to Own the Internet in Your Space Time, 2002, available at:
- Sulfab M 'Challenges of cybercrime in South Africa', research paper for Master of Arts in national security studies, American Military University (2014) 9.
- Swale, Voice Over IP: Systems and Solutions, 2001; Black, Voice Over IP, 2001.
The Budapest Convention on Cybercrime, opened for signature 23 November 2001, entered into force 1 July 2004
- The Constitution of Kenya, 2010, art 2(1)
- The Cybercrime and Computer Related Crimes Bill, 2014.
- The First African Forum on Cybercrime, October 16, 2018 to October 18, 2018, Addis Ababa Ethiopia
- The Internet Legislative and Policy Environment in Kenya report January, 2014
- The Internet Organized Crime Threat Assessment (IOCTA), 29 September 2014 Report
- The Kenya Information and Communications Act, 1998
- United Nations Conference on Trade and Development, Harmonizing Cyber laws and Regulations, the experience of East African Community, August 2013
- United Nations Economic Commission for Africa, Policy Brief, Tackling the Challenges of Cyber security in Africa
- United Nations Office on Drugs and Crime, Global Program on Cybercrime Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime, October 2019

Watney M, The Evolution of legal regulation of the Internet to address terrorism and other crimes' (2007) 3 *Tydskrif vir die Suid-Afrikaanse Reg* 469

Weber, Criminals may overwhelm the web, BBC News, 25.01.2007,

Wile J., "High-tech Crime: A New Type of Disaster", *Security Technology and Design* 47, Vol. 9 (1), January 1999, P72-75

www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

www.techweb.com/wire/172303160

Zsuzsanna Deen-Racsomány, 'Active personality and non-extradition of nationals in international criminal law at the dawn of the twenty-first century: adapting key functions of nationality to the requirements of International Criminal Justice' (2007) Doctoral dissertation, EM Meijers Institute of Legal Studies, Faculty of Law, Leiden University

APPENDICES

Appendix A: Questionnaire

My name is Bernard Barasa Walumoli a student at the National Defense College, an affiliate of the University of Nairobi in Kenya. I am undertaking a Master's degree in International Studies at the Institute of Diplomacy and International Studies (IDIS). I am conducting a study titled, "A Critical Analysis of the Challenges Facing Counter-Cybercrime in 21st Century Africa: A Focused Comparison of Kenya and Rwanda". This is in partial fulfillment of the requirement for the award of the Degree of Masters of Art at the Institute of Diplomacy and International Studies. Kindly note that all information gathered will be treated with strict confidentiality and will only be used for the purpose of this study. Kindly attempt all questions by either ticking () or putting a cross (X) on your selected choice. You may add any information you consider necessary in the space provided for each questions.

Section A: Demographic Data

1. Gender

Male ()

Female ()

2. Position/Designation

Executive ()

Senior Management ()

Middle Management ()

3. Highest level of Education

Primary Education ()

Secondary Education ()

Certificate/Diploma ()

Bachelor's Degree ()

Masters/ Degree ()

Others (Please specify):

4. For how long have you been in the service:

5. Which country do you come from:

6. Do you have Knowledge in counter cybercrime?

Yes ()

No ()

Appendix B: Interview/Questionnaire Guide for Respondents

1. Countering cybercrime in your country faces a number challenges.
A. Strongly agree ()
B. Agree ()
C. Disagree ()
D. Strongly disagree ()

2. What are the main challenges of countering cybercrime in your country?
.....
.....
.....
.....

3. Would you consider the difference in jurisdictions to be challenge in countering cybercrime?
Yes ()
No ()

4. Are there adequate legislations in your country to counter cybercrime?
Yes ()
No ()

5. How would you rate the level of enforcement mechanisms in countering cybercrime?
A. Very good ()
B. Good ()
C. Fair ()

- D. poor ()
6. Are there any challenges in identifying cybercrime criminals?
Yes ()
No ()
7. How difficult is it to collect evidence to prosecute cybercrime offences?
A. Very Difficult ()
B. Difficult ()
C. Ease ()
D. Very Ease ()
8. Are law enforcers in your country adequately trained to counter cybercrimes?
Yes ()
No ()
9. Are law enforcers in your country well remunerated to counter cybercrime?
Yes ()
No ()
10. In your opinion to what extend does different countries cooperate in counter cybercrime investigations?
A. Not at all ()
B. Less extend ()
C. Moderately ()
D. Large extend ()
E. Very large extend ()

11. To what extent does the current criminal laws and regulations cover cybercrimes?
- A. Not at all ()
 - B. Less extend ()
 - C. Moderately ()
 - D. Large extend ()
 - E. Very large extend ()
12. Are cybercrime laws and regulations in your country enforced to the letter?
- Yes ()
 - No ()
13. Counter cybercrime laws and regulations are uniform in all countries?
- A. Strongly agree ()
 - B. Agree ()
 - C. Disagree ()
 - D. Strongly disagree ()
14. High speed of data exchange process negatively affects cybercrime investigations.
- A. Strongly disagree ()
 - B. Disagree ()
 - C. Uncertain ()
 - D. Agree ()
 - E. Strongly agree ()

15. Kindly show the level of agreement or disagreement with respect to the following statements as they concerns counter cybercrime challenges in your country.

1. Strongly disagree 2. Disagree 3. Uncertain 4. Agree 5. Strongly agree

1 2 3 4 5

There is total legal and international cooperation in countering cyber crimes

Extradition is not a challenge in countering cybercrime

Readily available information on the internet is not a challenge in countering cybercrime

Readily available devices and Ease access of the internet are a challenge to countering cybercrime

Drafting National criminal laws adequately covers cybercrime

16. Does your country have proper mechanisms of monitoring and regulating the internet?

Yes ()

No ()

Not sure ()

17. How does your country ensure that cybercrime laws and regulations are adhered to?

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

24. What measures has your country put in place to deal with counter cybercrime challenges?

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

25. In your opinion what can be done to minimize the challenges faced in countering cybercrime?.....

.....
.....

Thank you very much for your responses