KIGALI INDEPENDENT UNIVERSITY ULK

SCHOOL OF LAW

DEPARTMENT OF LAW

P.O BOX 2289 KIGALI

LEGAL ANALYSIS ON THE PROSECUTION OF CYBER CRIMES IN EAST AFRICAN COMMUNITY [EAC]

Research proposal is submitted at school of law in partial fulfillment of the academic requirement for the award of bachelor degrees with honors in law prepared by:

NAME: MAYIIK DENG MAYIIK MEI

Roll Number: 202110021

SUPERVISOR: MURANGWA Eduard

Kigali, August 2024

DEDICATION

I dedicate this work to:

My family (My Parents, Brothers and Sisters)

My daughter Alang Mayiik Deng,

My heads of Family Deng Mayiik, Guk Nyok Koch, Nyanchath Kur Deng, Nyapiny Ruai Deng, Athieng Deng Mayiik, Nyok Deng Mayiik and the rest of my immediate family members.

My Supervisor, MURANGWA EDUARD

All my friends, Atak Tong Atak, Gatluak Yak Deng, Nyamiim Gai Nyamiim just a few to mention, colleagues and the entire LLB class of 2024

My mentor and friend Dr. Kabano Jacques

DECLARATION

I, MAYIIK DENG MAYIIK MEI, hereby declare that to the best of my knowledge the work presented in this dissertation entitled “LEGAL ANALYSIS ON THE PROSECUTION OF CYBER CRIMES IN EAC” is original and it has not been previously submitted elsewhere for any academic qualification. Any supportive materials used in terms of references from other persons’ works are found in the footnotes and in the bibliography.

Date: ……………………………………………………

Signature: ……………

DECLARATION BY SUPERVISOR

……………………………………………………………………………………………………
…………………..

Date: ……………………………………………………

Signature: …………

ACKNOWLEDGEMENTS

Upon the completion of this final project, I am pleasing the Almighty God for his blessing and grace in my daily life. So, I wish to express my heartfelt gratitude to all those who contributed to its completion. Through this view, I want to recognize the influence of my family members whose words of encouragement from the start of my life and assistance either morally or financially.

My head of family who had a vital influence on my academic life, and brothers and sisters, friends and families who helped directly or indirectly to achieve my work, I thank the authorities of the, KIGALI INDEPENDENT UNIVERSITY (ULK), specifically the School of Law for having put in place the module to transform theoretical knowledge into research practices. This enables me to attain a full research supervised for the fulfillment of a bachelor's degree. The same acknowledgment goes to my Supervisor MURANGWA EDUARD, for his kind supervision and help in terms of provision of certain materials and guidance as well as for undertaking the task to supervise my work. Without his excellent supervision, full of legal and crucial analysis for the sake of its completion, my work would not have been in the light of today. Lastly, I thank all persons who contributed and helped me in one way or another, either direct or indirect to achieve my light expectations in the KIGALI INDEPENDENT UNIVERSITY (ULK) throughout the academic period.

May God bless you all!

Table of Contents

LIST OF ACRONYMS AND ABBREVIATIONS

ADR: Alternative Dispute Resolutions

Art: Article

ATM: Automatic Teller Machine

EAC: East African Community

EACO: East African Community Organization Congress

I.e.: in other words

ICC: International Criminal Court

INTERPOL: International Criminal Police Organization

ITU: International Telecommunication Union

MLA: Mutual Legal Assistance

NCSA: National Cyber Security Authority

NICI: National Information and Communication Infrastructure plan

NISP: National Information Security Policy

NISS: National Information Security Strategy

No: Number

P: Page

Para: Paragraph

RIB: Rwanda Investigation Bureau

SS: South Sudan

USA: United States of America

Vol: Volume

GENERAL INTRODUCTION

Cybercrime is a complex issue with no internationally agreed-upon definition. Different states and organizations have their own criteria, leaving gaps between them, this lack of a widely accepted definition impacts jurisdiction, criminal prosecution, and the issue's scope, the prefix 'cyber', introduced in 1948, has lost its specificity, becoming commonly used to describe the perceived virtual environment associated with the Internet, this definition is too vague to accurately capture new criminal activities.[1]

Cybercrime, defined as criminal activity on computer networks and the Internet, has limitations. It is too narrow to include non-networking activities, such as connecting malicious software to a computer. It also broadens to include traditional crimes with only a small element tied to internet-based activity, such as murders planned using VoIP and Internet messaging applications, this classification is incorrect as it does not consider fundamental changes in criminal activity.[3]Cybercrime is not merely the use of technology in criminal acts, but it can be a new type of crime due to the digitization of information and decentralized file sharing services, the distinction between traditional crimes that involve technology but not alter the crime's nature and those that have been significantly augmented is debated, however, if a computer is the target or central tool in facilitating the act, it is considered a cybercrime.[4]

1. BACKGROUND OF THE STUDY

For the globe, cybercrime is a new kind of criminality. It is defined as any illegal omission that occurs on or through the internet, computers, or other technologies that the information technology act recognizes.[5] The most common crime that is destroying modern world is cybercrime, as consequences cybercrimes generating massive damages to the government and society; moreover criminals are also able to hide their identities from detection and technically proficient criminals use the internet to carry out a variety of illicit operations.[6] Expanding the

[1] ITU, Understanding cybercrime:Phenomenon, challenges and legal response, ITU Telecommunications development sector, (2012) P19.

[3] Kyoung S M et al, an International comparative study on cyber security strategy, an international journal of security and its application, vol 9, issue no 2 (2015) p 13

[4] Hunton, Paul, 'The growing phenomenon of crime and the internet: A cybercrime execution and analysis model', Computer Law and Security Review, 29, (2009) p. 529

[5] Prof. Chaubey R K, An Introduction to Cybercrime and Cyber Law, Kamal Law House, P 27 (2012). Available at https://www.bharatilawhouse.com/product/kamals-an-introduction-to-cyber-crime-and-cyber-law-r-k-chaubey-reprint-edition-2021/ accessed on 13 June 2024.

[6] Gorman L, Maclean D Media and Society in Twentieth Century, Blackwell publishing, 2003.

definition, cybercrime can be discussed as any unlawful acts in which a computer or the internet is used as a tool, a target, or both.[7]

Although the term "cybercrime" is always clearly defined case law adjudicated national court of member's states of EAC, it was interpreted judicially in some court decisions like in Uganda;[8] Kenya; Tanzania and other counties of the world like India.[9] Cybercrime is an uncontrollable evil that stems from the misuse of the increasing reliance on computers in contemporary society. The usage of computers and related technologies in daily life is expanding quickly; the internet and digital technologies have grown significantly and brought additional advantages to the government, investors, and citizens at large, then those digital technology and the internet have given rise to new forms of cybercrime such as phishing; online fraud, and hacking; widespread hazards to national security, business, and individual citizens are posed by the circulation and exploitation of illicit content and specifically cyberstalking, cyberterrorism, email spoofing, email bombing, cyber pornography, cyber defamation, and other recently developed cybercrimes.[10] Cyber criminality in EAC, often extending beyond national boundaries, necessitates a coordinated regional strategy for effective combat.[11]

In history EAC has established in 1917 by British colonial territory composed by KENYA, TANZANIA and UGANDA, they establish Custom Union followed by East African High commission in 1948and East African Common Service Organization in 1961.[12] However, we have to note that EAC was established by treaty of East African Cooperation signed by KENYA; UGANDA and TANZANIA in 1967. A number of political and economic factors led to the original EAC's collapse in 1977, the treaty for the establishment of the East African Community which was signed in 1999 and went into effect in 2000, brought the EAC back to life after many

[7] Prof. Chaubey R K, supra note 1.

[8] The Hon. Chief Justice of Uganda, Mr. Justice Benjamin Odoki, Justice for Everyone: a Myth or Reality? From the Ugandan perspective, p 18, Conference Report available at https://judiciary.go.ug/files/downloads/Justice%20For%20Everyone%20Myth%20or%20Reality.pdf accessed on 13 June 2024.

[9] Prof. Chaubey R K, supra note 2.

[10] Ibraham D et al, The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press, P 69-144, (2001). Available at https://books.google.rw/books/about/The_Transnational_Dimension_of_Cyber_Cri.html?id=SIcnAgAAQBAJ&redir_esc=y accessed on 13 June 2024.

[11] United Nations Conference on Trade and Development, East African Community, Draft EAC Legal Framework for Cyber Laws (2008)

[12] https://www.eac.int/eac-history

years.[13] The goal of the new EAC was to increase partner state collaboration and regional integration. Ever since it was resurrected, the EAC has grown and changed dramatically where different partner states joined the community like Burundi, Republic of Rwanda, Somalia; Democratique Republic of Congo and South Sudan.[14] The East African Court of Justice, the East African Legislative Assembly, and the East African Customs Union are just a few of the organizations that the EAC has founded.

Those partner states have acknowledged the significance of tackling cyber security risks and adopted the EAC Cyber Security Framework serves as a basis for collaboration and the development of capability in this field.[15] Due to the complexity of these crimes, jurisdictional concerns, and the absence of uniform legal frameworks among EAC member states, cybercrime prosecutions continue to pose a serious difficulties and challenges.

2. INTEREST OF THE STUDY

This study is comprised by personal, academic, and scientific interests; the study on the legal analysis of cybercrime prosecution in the EAC can contribute to protecting individual rights, advancing scholarly discourse, and informing policy and practice in combating cyber criminality at the regional and international levels.

2.1. Personal interest

This study draws attention to the alarming rise in cybercrimes, such as fraud and identity theft, and the study provide detrimental effects these crimes have on people, companies, and society as a whole. Thesis examines the importance of harmonizing cybercrime laws in the EAC to protect the rights and interests of individuals and businesses .It recommends bolstering the EAC region's prosecution strategies.

2.2. Academic interest

This study is important from an academic standpoint since it tackles a modern and developing area of law that interacts with technology, security, and regional cooperation. It adds to the expanding corpus of knowledge on the prosecution of cybercrimes, harmonization of the law, and the difficulties judicial systems have in adjusting to the digital era. The study findings can influence future research in this area as well as legal education and intellectual discourse as it has

[13] https://www.eac.int/overview-of-eac

[14] African Union Commission, 2019 African Regional Integration Report, Towards an Integrated Prosperous and Peaceful Africa, p 19-28 (2019) available at

[15] United Nations Conference on Trade and Development, East African Community, Draft EAC Legal Framework for Cyber Laws (2008)

revealing the academic relevance of studying cybercrime prosecution in the EAC context, particularly in relation to legal harmonization and regional cooperation.

2.3. Scientific interest

This study has scientific interest as it employs a systematic and rigorous approach in analyzing legal frameworks, judicial practices, and regional cooperation mechanisms related to cybercrime prosecution in the EAC. The findings can contribute to the broader understanding of the challenges and potential solutions in combating transnational cybercrimes, which has implications for policy development, capacity building and international cooperation efforts.

3. DELIMITATION OF THE STUDY

The topic stands as the legal analysis on the prosecution of cybercrime in East African Community, it would be limited in space under the territory of EAC member states, in domain the study has to deal with criminal law by analyzing the cyber-crime as unlawful act from its prosecutions to its convictions in EAC and about delimitation in time, the study analyses current state of cybercrime in the regions of EAC.

3.1. Delimitation in space

The study is delimited to the East African Community (EAC) region, which includes partner states such as Kenya, Uganda, Tanzania, Burundi, Rwanda, South Sudan, Federal of Somalia and the Democratic Republic of Congo. The study focuses on the legal frameworks, challenges, and mechanisms related to the prosecution of cybercrimes within the geographical boundaries of the EAC member states.

3.2. Delimitation in domain

The study is delimited to the domain of criminal law, specifically addressing the prosecution of cybercrimes within the EAC. It will examine the existing legal instruments, judicial practices, and regional cooperation mechanisms established by the EAC to combat cybercrimes. The study will focus on analyzing the legal and practical challenges faced in investigating, prosecuting, and adjudicating cybercrimes, with a particular emphasis on those cybercrimes with cross-border elements.

3.3. Delimitation in time

This study will focus on the current state of cybercrime prosecution in the EAC and the challenges faced in recent years. However, it may also consider the historical evolution of the EAC's efforts to address cybercrime and the development of relevant legal frameworks over time.

The study may also consider recent developments, trends, and emerging issues related to cybercrime prosecution within the EAC region.

4. PROBLEM STATEMENT

East African Communities put efforts to enhance cyber security but the prosecution of cybercrimes within the region continues to face numerous obstacles like the lack of harmonized laws and regulations among the partner states; inadequate technical and legal expertise in cybercrimes which challenge the effectiveness of investigation; prosecution and adjudication of cyber-related offenses.[16] The cybercrimes with cross-border element introduce difficulties relating with jurisdiction, extradition and mutual legal assistance which further complicating the prosecution process.[17] Even if the EAC's efforts to address cyber security threats through the adoption of frameworks like the EAC Cyber Security Framework,[18] the prosecution of cyber-crimes within the region remains a significant challenge and the lack of harmonized legal frameworks, inadequate technical and legal expertise, and jurisdictional complexities arising from the cross-border nature of many cyber-crimes impede effective investigation, prosecution, and adjudication of these offenses.[19] Specifically, this study will try to elaborate major challenges faced by law enforcement agencies and judicial systems in the EAC when investigating, prosecuting, and adjudicating cybercrimes, particularly those with cross-border elements which have to be settled through harmonizing cybercrime laws in the EAC to protect the rights and interests of individuals and businesses.

According to the technological developments cyber-security issues are now a global problem with many facets, improving and maintaining cyber-security is now a top priority for both national and international politics.[20] Governments have to play a significant role in international politics by providing services to guarantee citizens' safety both offline and online.[21] Since cyber threats have an international scope, it is ineffective to concentrate resources solely on national defense. Cybercriminals typically operate from nations with lax rules, targeting even those with

[16] Marco, G. Understanding Cybercrime: Phenomena, Challenges and Legal Response (Ed)(2012), pp.1 and 71

[17] Marco, G, supra note 1, p 64

[18] United Nations Conference on Trade and Development, East African Community, Draft EAC Legal Framework for Cyber Laws (2008)

[19] Majamba H L et al Harmonization of cybercrime legal frameworks within East African Community , University of Dar-es-Salaam School of Law P 7-9.

[20] Chimilila C et al Trade Facilitation in EAC Customs Union: Its Achievement and Implementation in Tanzania, Journal Of Economics and Sustainable Development, (2014), Vol. 5, No.25, pp. 4 - 5.

[21] Athina, K., (2008), 'Introduction: New Media and the Reconfiguration of Power in Global politics' in KaratzogianniAthina (Ed), Cyber Conflict and Global Politics, Routledge, pp. 3 – 5

strict cyber regulations[22], it has been observed that attempts to stop this cybercrime have not been successful For instance, the speed at which online platforms are developing and the need for creative solutions to match their complexity have made the offline mutual legal aid agreements that certain States have entered into ineffective.[23] As a result, regional and international legal initiatives addressing cyber-related issues particularly those related to cybercrimes and cybersecurity need to be harmonized. The East African Community (EAC) must address cyber-security concerns at the national level and address the harmonization of cyber laws in order to address the international aspect of these challenges if it is to ensure the strengthening of regional integration and address the welfare of its citizens.

5. RESEARCH QUESTIONS

1. What are the major challenges faced by law enforcement agencies and judicial systems in the EAC when investigating, prosecuting, and adjudicating cybercrimes, particularly those with cross-border elements?

2. What are the legal and institutional mechanisms that can be adopted for effective transformation of cybercrimes in EAC?

6. RESEARCH HYPOTHESIS

1. The prosecution of cybercrime in EAC are not effective due lack of harmonized legal framework, lack of well-trained enforcers on the cybercrime, lack of enough resources and others,[24]

2. Institutional and legal mechanisms can be instituted to ensure effective prosecution of cybercrime in EAC.

7. RESEARCH OBJECTIVES

The study has both general objective and specific objectives, as it aimed to criticize the laws and obstacles that hinder the effective prosecution of cyber-crime in EAC, and it will relate specific objective with research questions by revealing the challenges faced by prosecutors, and judicial systems in the EAC when investigating, prosecuting, and adjudicating cybercrimes, particularly

[22] UNCTAD Harmonizing Cyber Laws and Regulations: The Experience of the East African Community, United Nations, New York, (2013), p. 6, available at: https://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf. Accessed at 14th June 2024

[23] Achieng, R. Expert Meeting on Cyberlaws and Regulations for Enhancing E-Commerce: Including Case Studies and Lessons Learned, (2015), available at: https://unctad.org/meetings/en/Presentation/CII_EM5_P_RAchieng_en.pdf, accessed on 14th June , 2024.

[24] Fafinski, et al Mapping and Measuring Cybercrime', OII Forum, Paper No 18, (2010) p. 11

those with cross-border elements, and propose mechanisms to be enforced as the way of overcoming those challenges.

7.1. General objectives

The purposes of this study is critically analyzing the legal frameworks and challenges surrounding the prosecution of cybercrimes within the East African Community (EAC), the thesis hunt through the existing legal instruments, judicial practices, and international cooperation mechanisms and identify gaps which hinder the combating cyber criminality effectively. The study aims to provide a comprehensive analysis of the legal and practical challenges in prosecuting, investigating an adjudicating cybercrimes in the EAC region and in the end this study will propose while propose potential solutions and strategies for enhancing regional cooperation and harmonization efforts to combat cyber criminality effectively.

7.2. Specific objective

1. To identify the key challenges faced by law enforcement agencies, prosecutors, and judicial systems in the EAC when investigating, prosecuting, and adjudicating cybercrimes, particularly those with cross-border elements.

2. To propose recommendations for strengthening the legal and institutional frameworks, as well as regional cooperation mechanisms, to enhance the prosecution of cybercrimes within the EAC, and to elaborate the importance of harmonizing cybercrime laws in the EAC as the way of responding to the mentioned challenges and protect the rights and interests of individuals and businesses

8. RESEARCH METHODOLOGY

Research methodologies is a methods used in a specific type of inquiry that is conducted in the presence of an issue that needs to be resolved or a question that needs to be addressed, research is always hedged about with uncertainty and risk, research is a part of a wider process that constitutes and renders a subject, amenable to study in a distinctive way. However, it is concerned with seeking solutions to problems or answers to questions.[25]

8.1. Research Techniques

During this study the following techniques will be used in the way of collecting information as documentary techniques because it is most important in providing accurate information which is

[25] Ahmed U J, Documentary research methods: New dimension, Indus journal of Management and social science, vol 4, issu no 1 (2010) p 1-14

suitable on the legal analysis to the prosecution of cybercrime in EAC.A document is a written text that must be studied as socially situated products, distinct from records prepared for specific investigator requests. Documentary research goes beyond recording facts and involves a reflexive process that confronts the moral underpinnings of social inquiry. Documents need a theoretical frame of reference to understand their content and are crucial sources of information in social research.[26]

8.1.1. Documentary technique

Documentary technique is a research conducted in the way of using official document or personal document as source of information, through this documentary technique the study will employ Documentary Review by using different techniques such as empirical methodologies, documentary research, and qualitative data analysis.[27] This documentary review will involve analyzing various types of documents related to the prosecution of cybercrimes in the EAC region, doctrinal method which is traditionally the main methodology of legal research will be employed to review literature on the administration of justice, particularly the legislative system. This method focuses on examining what the law is, rather than what it ought to be.[28] Primary data for the study will be obtained from legislations or laws, through desk review which means that the researcher will collect and analyze relevant laws, regulations, and policies related to cybercrime prosecution in the EAC member states.

The legal status analysis under the doctrinal methodology, the study will locate and collect the applicable laws[29] and apply them to the specific set of facts related to the prosecution of cybercrimes in the EAC. It will enable revealing the current legal status of cybercrimes in the EAC region, based on the laws in force through the acts of the community. In the Problem Identification the documentary technique will help the researcher identify gaps or problems in the existing legal frameworks by examining the root causes of the challenges faced in prosecuting cybercrimes within the EAC.

[26] Ahmed U J, supra note 1, p 10

[27] Makulilo, A.B, Protection of Personal Data in sub-Saharan Africa, PhD Thesis, University of Bremen, Germany, 2012 at p.52.

[28] McGrath, J.E. Methodology Matters: Doing Research in the Behavioural and Social Sciences, in Baecker, R. M. et al. (1995). Readings in Human-Computer Interaction: Toward the Year 2000, Morgan Kaufmann Publishers, p. 154, as quoted in Makulilo, A, B., note 124. See also, Singhal, A. K. and Malik, I, Doctrinal and Social Legal Methods: Merits and Demerits, Educational Research Journal, 2012, Vol.2, No.7, pp.252-256, at p. 252

[29] McGrath, J.E. supra note 1.

8.2. Research methods

During this study the following methods of analytical and exegetic methods will be employed to collect information for the issue of elaborating the research problem of this study in details.

8.2.1. Analytical method

This analytical method is defined as breaking down complex information into smaller components to achieve a better understanding of the whole information.[30] Through the use of an analytical method, this study will examine the legal frameworks currently in place by examining the cybercrime laws, regulations, and policies of the EAC member states in order to identify similarities, differences, strengths, and weaknesses in their approaches to dealing with cybercrimes. Additionally, the study will examine judicial practices by analyzing court decisions, case laws, and judicial interpretations related to cybercrime prosecution in the EAC region. This will help to reveal the practical challenges faced by the judicial systems and how they have resolved. Finally, the study will evaluate regional cooperation mechanisms like mutual legal aid treaties work to support cross-border cybercrime investigations and prosecutions inside the EAC.

8.2.2. Exegetic method

An exegetic method refers to the critical interpretation and elucidation of the significance and ramifications of written materials, including legal documents, statutes, and regulations.[31] The purpose of this study is to interpret the legal provisions of cybercrime laws and regulations of the member states of the Eastern African Community (EAC), providing clarification on their applicability, extent, and possible ambiguities. It will investigate the legislative intent. It will be possible to understand the purpose and goals of the cybercrime legislation that the EAC has enacted by looking through the legislative background, preparatory studies, and discussions surrounding their passage. This study would thus provide for a more thorough understanding of the legislative frameworks controlling cybercrime prosecution within the larger socio-economic, political, and technological landscapes of the EAC member nations.

8.2.3. Synthetic method

Synthetic method of research is a set of related methods that integrate the findings of separate empirical studies, it is a tool for understanding a body of literature and characteristics that enhance or diminish relationship of interest.[32] Synthetic methods of research, in the context of

[30] Makulilo, A.B, supra note 1.

[31] McGrath, J.E. supra note 2.

[32] Rebeca R S et al, Research synthesis Methods, Texas state University (2022) p 17

legal studies, involve combining and integrating various sources, approaches, and findings to create a comprehensive understanding of a complex issue. This methodology goes beyond merely analyzing individual components; it seeks to synthesize diverse information to form new insights and holistic perspectives. In legal research, synthetic methods often involve merging theoretical frameworks with empirical data, combining qualitative and quantitative approaches, and integrating insights from multiple jurisdictions or legal systems.[33] This approach is particularly valuable when dealing with multifaceted issues that span different areas of law or cross national boundaries. Synthetic methods of research are beneficial for analyzing the prosecution of cybercrime in the EAC, as it involves multiple layers of complexity. This approach integrates analyses of member states' legal frameworks, regional cooperation mechanisms, technological challenges, and international best practices, identifying gaps, proposing harmonized approaches, and suggesting innovative strategies for East Africa's unique cybercrime context.

9. SUBDIVISION OF THE STUDY

This study composed by only three chapters, where general introduction will comprise background of the cybercrimes all over the world and historical evolution of EAC; the interest of the study for personal, academic and for scientific; the scope of the study by elaborating the scope in space, scope in domain and the scope in time; the statement of problem; the research questions; research hypotheses; research objectives both general and specific objectives; the research methodologies with research techniques of documentary techniques, research methods of analytical and exegetic methods.

Chapter 1, will be made of conceptual and theoretical framework by emphasizing in defining different key terms of this study, chapter 2, will be composed by elaborating research problem in details, this chapter will elaborate more on the challenges faced by law enforcement agencies and judicial systems in the EAC when investigating, prosecuting, and adjudicating cybercrimes, particularly those with cross-border elements and chapter 3, which is last but not least will combine all mechanisms to be adopted by law enforcers to handle such elaborated challenges in previous chapter.

[33] Rebeca R S et al, supra note 1, p 20

CHAPTER1: CONCEPTUAL AND THEORETICAL FRAMEWORK

This chapter includes definition of key terms specifically, cybercrime, jurisdiction, digital evidence, mutual legal assistance (MLA), data protection and cybersecurity, general overview for cybercrime in East African community, element of cybercrimes, theories related to legal and judicial systems and short history of EAC.

1.1. Definition of key terms

The following are definition of key terms relating with this study:

1.1.1. Cybercrime

Cybercrime refers to criminal activities which took place by using computer, digital devices, or computer networks as the primary means of committing an offense, it include the different illegal activities such as hacking, identity theft, online fraud, and the distribution of malicious software. Or cybercrime is defined as an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites, and technology or facilitate a crime.[34]

1.1.2. Jurisdiction

Jurisdiction In the way of cybercrime prosecution, jurisdiction refers to the legal authority of a court or law enforcement agency to try and determine cases related to cybercrimes. According to the transnational nature of cybercrime the determination of jurisdiction may be difficult because always it is challenged by some barriers like knowing where the crime was committed, where the perpetrator is located, and where the victims are situated.[35]

1.1.3. Digital Evidence

Digital Evidence is composed by different information stored or transmitted in digital form that may be used as evidence proceedings; it includes data from computers, mobile devices, networks, and cloud storage. Sometimes the admissibility and handling of digital evidence are crucial aspects of cybercrime prosecution, requiring specific procedures to ensure its integrity and authenticity.

1.1.4. Mutual legal Assistance

Mutual Legal Assistance (MLA) it is an agreement between two or more state by accepting on how they will work together in gathering and exchanging information to enforce laws, according

[34] Zaidy A A, Digital crime and our society, Academia Letters (2022), p 2.

[35] Maujili, jurisdictional challenges in fighting cybercrimes: any panacea from international law? (2015) p 57.

to the agreement one state may request and provide assistance to other state, in cybercrimes this mutual legal assistance is important as it enable state obtaining evidence across borders through interviewing witnesses in foreign jurisdictions, and facilitating extradition of suspects.

1.1.5. Harmonization

Harmonization of Laws is the process of aligning legislation across the member state of a given community to ensure its consistency in definitions, penalties, applicability or enforcement procedure. This harmonization of laws result to the effectiveness of regional co-operation in combating crime specifically those committed under the cyber space.[36]

1.1.6. Data protection

Data Protection is the way of adopting legal and regulatory framework with the aim promoting the privacy and security of personal information. For the issue of cybercrime data protection laws are important as investigators must balance the need to gather evidence with the obligation to respect individuals' privacy rights.[37]

1.1.7. Cybersecurity

Cybersecurity encompasses the practices, technologies, and processes established to protect networks, devices, programs, and data from attack, damage, or unauthorized access. In the context of cybercrime prosecution, adoption of cybersecurity measures is necessary for both preventing crimes and investigating breaches.[38]

1.1.8. Dark web

The dark web is a subset of the deep web, intentionally hidden and inaccessible through standard web browsers. Accessing it requires specialized software and authorization. The Onion Router (Tor) network is the most common tool for accessing the dark web, it operates on overlay networks using public internet infrastructure but requires specific protocols.[39]

[36] DR. ADEL AZZAM S H, Jurisdiction in Cybercrimes: A Comparative Study, Journal of Law, Policy and Globalization, vol 22, (2014),p 75-80. Available at https://core.ac.uk/download/pdf/234649797.pdf acessed on 03 July 2024.

[37] Schjolberg S & Ghernaouti-Hélie S, A Global Protocol on Cybersecurity and Cybercrime, Cybercrimedata(2009)p4

[38] Prof. Sharma P, A Review of International Legal Framework to Combat Cybercrime, nternational Journal of Advanced Research in Computer Science, Vol 8, issue No. 5, (2017), p 1372.

[39] Prof. Sharma P, supra note 1, p 1370

1.1.9. Hacking

Hacking is the unauthorized access, manipulation, or exploitation of computer systems, networks, or digital devices, it involves technical skills to bypass security measures and gain access to protected data, hackers use techniques like social engineering, malware deployment, network infiltration, and cryptographic attacks, malicious hacking is criminal, aiming to steal sensitive information or cause financial harm, as technology evolves, it challenges cybersecurity professionals and law enforcement agencies.[40]

1.1.10. Phishing

Phishing is a type of cybercrime where attackers attempt to deceive individuals into revealing sensitive information such as login credentials, financial details, or personal data by masquerading as a trustworthy entity in electronic communication, this fraudulent practice typically involves sending emails, text messages, or creating fake websites that appear to be from legitimate sources to trick recipients into providing confidential information or clicking on malicious links.[41]

1.1.11. Identity Theft

Identity theft is a cybercrime where personal or financial information is obtained and used without authorization, often for financial gain or fraud. It's prevalent in the digital age, with methods like phishing scams, data breaches, and theft of physical documents. Victims can suffer severe financial losses, damaged credit scores, and a time-consuming process to reclaim their identity. In the East African Community, it presents significant challenges for law enforcement and legal systems.[42]

1.1.12. Cyber Terrorism

Cyber terrorism refers to the use of digital technologies and networks to conduct terrorist activities or to support terrorist organizations; it involves politically or ideologically motivated attacks against information systems, computer networks, and technological infrastructure to cause fear, disruption, or physical harm.[43]

[40] Snail S, cybercrime in South Africa, hacking, cracking and other unlawful online activities, journal of information, law & technology, vol 1, (2009) p 61

[41] Snail S, supra note 1, p 70

[42] Hoofnagle C J, Identity theft: Making the kown unknowns known 2007 Harvard Journal of Law & Techinology, vol 21, (2007)p 113.

[43] Ashiru A, identifying phishing as form of cyber-crime in Nigeria, Department of Public and Private Law, Lagos State University, Lagos-Badagry Expressway vol 12, issue no 2(2021) p 120

1.1.13. Transitional crime

Transnational crime, particularly cybercrime, involves activities that cross national borders, affecting multiple countries or jurisdictions; this phenomenon is increasingly prevalent in the digital age, with advanced technologies enabling criminals to operate across geographical boundaries. Addressing transnational cybercrime requires robust international cooperation, harmonized legal frameworks, and sophisticated cross-border investigative techniques, particularly within regional blocs like the East African Community. Traditional jurisdiction and sovereignty concepts often fail to address these complex crimes.[44]

1.2. The concept of cybercrime

The cyber-crime as any activity that took place in a computer, network or networked device where a cybercriminals use cybercrimes to generate income, most of cyber-crimes are committed against computers or devices to directly damage or disable them. The Internet and the World Wide Web have revolutionized the digital environment, enabling individuals to express their needs and feelings.[45] Governments have established regulations to ensure secure networks and privacy, but this freedom may lead to individuals breaking these rules for various reasons, such as identity theft or scams. individuals and groups utilize the internet as a means of carrying out their criminal activities in order to further their ideology, which is supported by governments and terrorist organizations, digital terrorism and cybercrimes will be covered in this study because it is a prominent issue that has an impact on people's daily life specifically on the region of East African Community.[46] The risk of being attacked has increased significantly due to the massive growth of social networking, freedom of expression, and the ability to express one's own opinions on these websites and applications, via these social networking platforms, criminals have an easy place to launch attacks and target individuals, hacking and terrorist groups utilize the internet, including social networking sites, to communicate, exchange ideas, and plan their targets' whereabouts.[47]

[44] Stevenson R L B, 'Plugging the "Phishing" Hole: Legislation versus Technology', 5 Duke Law & Technology Review, (2005) p1-14.

[45] Dentzel Z, How the internet has changed everyday life, OPENMIND BBVA, p7. Available at https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/ accessed on 03 July 2024.

[46] Cassim F, Protecting personal information in the era of theft: just how safe is our personal information from identity thieves? Vol 18, issue no 2, (2015), p68.

[47] Doyle S, Cybercrime and violent crime are converging: here how to deal with it, World Economic Forum, (2023), p 25. Available at https://www.weforum.org/agenda/2023/10/cybercrime-violent-crime/ accessed on 03 July 2024.

1.2.1. Element of cybercrime

Cybercrime as like other criminal offence has both mental element (mens rea) and material element (actus reus).

1.2.1.1. Mental element (mens rea)

The mental element of cybercrime or mens rea, it is the state of mind or intent of the perpetrator when committing the offense, all of jurisdiction around the world, cybercrime laws require proof of intent to determine criminal liability, here involves the presenting that, accused acted knowingly, willfully, or with a specific purpose to cause harm or gain unauthorized access. As an example, in cases of unauthorized access to computer systems, prosecutors must prove that the accused intentionally accessed the system without permission of owner, knowing that such access was prohibited.[48] Sometime the level of intent required may be different according to the specific offense and jurisdiction. Some cybercrimes may require proof of specific intent, such as the intent to defraud in cases of online financial crimes.

1.2.1.2. Material element (actus reus)

The material element of cybercrime or actus reus, is composed by physical acts or omissions that constitute crime, for cybercrime, it involves actions taken through digital means, such as entering commands into a computer, transmitting data, or manipulating electronic systems, the actus reus must be voluntary and under the control of the perpetrator. For stance, material elements in cybercrime include unauthorized access to computer systems, interception of electronic communications, or the creation and distribution of malicious software, like in a case of illegal data interception, the actus reus might involve the use of software or hardware to capture network traffic without authorization. In a cyberstalking case, the material element could include sending threatening messages or repeatedly accessing the victim's online accounts.[49]

1.3. Theories related to legal and judicial systems

For the theories relating with legal and judicial system relevant to the East African Community, the study tried to briefly analyses transnational legal process theory, the deterrence theory and legal pluralism theory by elaborating on how those theory may be important in combating cybercrime in EAC.

[48] Anon, Cybercrime-prosecution guidance, https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

[49] United Nations, Comprehensive study on cybercrime, United Nation Office on Drug and crime, (2013) , p11-23.

1.3.1. Transnational legal process theory

Transnational legal process theory in the context of cybercrime prosecution given the cross-border nature of many cyber offenses, this theory dealt with how international and domestic legal norms are adopted, interpreted, and internalized by different stakeholders, accordingly, this theory may inform efforts to develop regional cybercrime laws and procedures that are compatible with international standards while respecting national sovereignties. It also provides a framework for understanding how member states can collaborate effectively in investigating and prosecuting cybercrimes that span multiple jurisdictions.[50]

1.3.2. Deterrence theory

Deterrence theory, derive its source in the criminal justice studies, it provide that the threat of punishment can discourage individuals from committing crimes,[51] in the realm of cybercrime prosecution in the EAC, this theory encourage to put efforts in establishing strict penalties for cyber offenses, the prediction is that potential cybercriminals will be less likely to engage in illegal activities if they perceive a high risk of detection and severe consequences. However, the application of deterrence theory to cybercrime faces challenges due to the anonymous and borderless nature of many cyber offenses, requiring the EAC to consider innovative approaches to enhance the deterrent effect of cybercrime laws.

1.3.3. Legal pluralism

Legal pluralism recognizes the coexistence of multiple legal systems within a single social field like in regional organization,[52] this theory acknowledges the diverse legal traditions present in the region, including common law, civil law, and customary law systems, in addressing cybercrime, EAC member states must navigate this pluralistic landscape, reconciling traditional legal approaches with the need for modern, technology-oriented laws and legal pluralism theory can inform strategies for developing cybercrime legislation that is both effective and culturally sensitive within the diverse EAC context.

[50] Alexandra P G, Transnational cyber offences, overcoming jurisdictional challenges, the yale journal of international law, vol 43, (2018) P 195.

[51] Johnson B, Do criminal law deters crime? Deterrence theory in criminal justice policy: A primier, MN House Research, (2019) P 17. Available at https://house.mn.gov/hrd/pubs/deterrence.pdf accessed on 03 July 2024.

[52] Merry S E, Legal pluralism, Law and society Review, vol 22, issue no 5, (1988) p869-896. Available at https://www.ojp.gov/ncjrs/virtual-library/abstracts/legal-pluralism accessed on 03 July 2024.

1.3.4. Universal jurisdiction

Universal jurisdiction, applicable to piracy offenses, addresses territorial jurisdiction issues by allowing international criminal tribunals to claim jurisdiction over an accused, regardless of the crime's location, this approach allows for prosecution of piracy under the United Nations Convention on the Law of the Sea (UNCLOS) and customary international law, cyber criminals can also be considered hostis humani generis, as cyberspace is considered the "high seas.[53] The D.C. Circuit Court of Appeals ruled that aiding and abetting piracy does not need to occur on the high seas to be illegal under UNCLOS, and universal jurisdiction for transnational cyber offenses should not be precluded by the fact that some countries may have jurisdiction,[54] universal jurisdiction over piracy and transnational cyber offenses like DDoS and ransomware could be justified due to their potential to endanger international trade and disrupt international corporations.[55]

1.3.5. Complementarity between member states domestic courts and ICC

The International Criminal Court (ICC) relies on complementarity, which allows domestic courts to exercise jurisdiction over international crimes, respecting state sovereignty and potentially encouraging states to join agreements like the Rome Statute.[56]The complementarity principle in cybercrime prosecution at the International Criminal Court (ICC) addresses territorial jurisdiction issues, if a country cannot prosecute a case domestically, it can try it before the ICC, a time limit is set for prosecution, and if not taken, the victim state can request the ICC prosecutor to press charges, complementarity also encourages countries to adopt transnational cyber offense legislation, the ICC's jurisdiction is primarily limited to ratifying States, which can refer cases involving alleged crimes committed by a national or territory of that State.[57]

[53] Higgins R, problems and process: International law and how we use it, oxford public international law, (1995)

[54] United States v. Ali, 718 F.3d 929, 935-38 (D.C. Cir. 2013). But see id. at 937 (strongly suggesting that "a facilitative act need not occur on the high seas so long as its predicate offense has" (emphasis added))

[55] See, e.g., United States v. Yousef, 327 F.3d 56, 104 (2d Cir. 2003) (citing "the threat that piracy poses to orderly transport and commerce between nations" as a basis for universal jurisdiction for piracy); Yvonne M. Dutton, Bringing Pirates to Justice: The Case for Including Piracy Within the Jurisdiction of the International Criminal Court, 11 CHI. J. INT'L L. 197, 204 (2010) ("It is the general heinousness of piratical acts and the fact that they are directed against ships and persons of many nationalities—disrupting international trade and commerce—that warrants universal jurisdiction.")

[56] Art. 5(1), Rome Statute of the International Criminal Court July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute].

[57] Art 12, In addition to jurisdiction over the nationals of a State party or over crimes committed on the territory of a State party, the ICC can also exercise jurisdiction over any individual when the Security Council refers a case to the Prosecutor under Chapter VII of the Charter of the United Nations. Id. Art. 13(b)

1.4. SHORT HISTORY OF EAC

The East African Community was established in 29th century by only three state namely Uganda, Kenya and Tanzania around 1967, this community declined in 1977 according to the political and economic reasons like lack of willing to pay contribution, revolutions in some state, conflict of leadership and lack of civilization for some actors in EAC, after that EAC was resurrected in 2000 only by these three state, Uganda, Kenya and Tanzania.[58]

Around 2007, Rwanda and Burundi joined community and members expand to five (5) members, after that Democratic Republic of Congo and Somalia had also joined community then the last member was South Sudan which was admitted in 2016.in the mission of EAC there are economic, political, social and cultural integration among its member state to promote quality life for people of East Africa. EAC designed to achieve those missions through increase competitiveness, value added production, promoting free trade in the region and free investment, the union aims to establish custom union, a common market, a monetary union and political federation of East African States.[59]

1.4.1. Kenya

Section 20(1) of the Kenyan Cybercrimes Act establishes an enhanced penalty for (i) unauthorised access, (ii) access with intent to commit a further offence, (iii) unauthorised interception and (iv) unauthorised interference, where these are committed on a 'protected computer system[60]

The Kenyan Cybercrimes Act clarifies in its explanatory memorandum the intention of its drafters to provide for offences related to computer systems; to enable timely and effective detection, investigation and prosecution of computer and cybercrimes; to facilitate international cooperation in dealing with computer and cybercrime matters; and for connected purposes’.

The Kenyan Cybercrimes Act has two closely related aims:

to protect the confidentiality, integrity and availability of computer systems, programs and data and to facilitate the detection, investigation, prosecution and punishment of cybercrimes.

[58] East African Community, 'History of the EAC' https://www.eac.int/eac-history accessed 3 July 2024.

[59] East African Community, supra note 1

[60] https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2023-03/D19156-CCJ-1-1-Kenya-Cybercrime-Law-Review--Sang-Sang.pdf

Key Provisions: Criminalizes offenses like unauthorized access, identity theft, and cyberbullying.

Implementation: Establishes a National Cybersecurity Coordination Centre to oversee implementation and response strategies.

Data Protection: Works in conjunction with the Data Protection Act, 2019, ensuring that data privacy rights are respected

1.4.2. Rwanda

The prosecution of cybercrimes in Rwanda has become increasingly significant as the country advances in digital technology and internet usage. Here are some key aspects of how Rwanda approaches the prosecution of cybercrimes:

1.4.4. Legal Framework

Cybersecurity Law: Rwanda has established a legal framework to combat cybercrime, notably the Law No. 60/2018 of 22/08/2018 on the Prevention and Punishment of Cybercrime. This law outlines various offenses related to cybercrime, including hacking, identity theft, and the dissemination of harmful content.

Data Protection Law: The law on the protection of personal data also plays a role in prosecuting cybercrimes, particularly those involving unauthorized access to personal information.

International Treaties: Rwanda is a signatory to several international treaties, such as the Budapest Convention on Cybercrime, which facilitates international cooperation in the prosecution of cyber offenses.

1.4.5. Enforcement Agencies

1. **Rwanda National Police (RNP)**: The RNP has specialized units dedicated to cybercrime. These units are trained to investigate, gather evidence, and collaborate with other agencies.
2. **Rwanda Utilities Regulatory Authority (RURA)**: This body oversees telecommunications and has a role in enforcing regulations that pertain to internet service providers and online content.
3. **Cybersecurity Task Force**: The Rwandan government has established a task force that coordinates efforts among various stakeholders to enhance cybersecurity and respond to cyber incidents.

Prosecution Process

Investigation: When a cybercrime is reported, the RNP’s cybercrime unit initiates an investigation, collecting digital evidence and working to trace the perpetrators.

Collaboration: Investigations often involve collaboration with international law enforcement agencies, especially in cases that cross borders.

Legal Proceedings: Once sufficient evidence is gathered, the case is brought before the courts. The prosecution must prove the elements of the offense beyond a reasonable doubt.

1.4.6. Recent Developments

Rwanda continues to strengthen its approach to cybercrime through various initiatives, including:

Capacity Building: Training programs for law enforcement and judiciary personnel to improve their understanding of cyber laws and investigative techniques.

Public Awareness Campaigns: Programs aimed at educating the public about the risks associated with online activities and the importance of cybersecurity.

Partnerships: Collaborating with international organizations and other countries to share best practices and improve the country’s cybercrime response[61].

1.4.7. Uganda

The prosecution of cybercrimes in Uganda has gained prominence as the country experiences rapid digitalization and increased internet penetration. The government has recognized the importance of addressing cyber threats to protect individuals, businesses, and national security. Here’s an in-depth look at the various aspects of how Uganda approaches the prosecution of cybercrimes:

1.4.8. Legal Framework

Cybersecurity Act (2021): The primary legislation governing cybercrime in Uganda is the Cybersecurity Act, which outlines offenses related to computer systems, data, and networks. This Act establishes legal definitions, penalties, and enforcement mechanisms for various cybercrimes, including hacking, data breaches, and unauthorized access to computer systems.

Computer Misuse Act (2011): This earlier legislation criminalizes offenses such as unauthorized access to computer systems, cyber harassment, and the distribution of harmful software. It provides a foundation for prosecuting many cyber-related offenses.

[61] file:///C:/Users/HP/Downloads/Law%20on%20Prevention%20and%20Punishment%20of%20Cybercrimes%20(4).pdf

Electronic Transactions Act (2011): This Act facilitates electronic transactions and lays down provisions for e-signatures, digital contracts, and electronic evidence, which can be crucial in cybercrime prosecutions.

Data Protection and Privacy Act (2019): This legislation protects personal data and privacy, addressing issues related to unauthorized data collection, processing, and dissemination.

International Treaties: Uganda is a member of various international organizations and treaties, including the African Union's Convention on Cyber Security and Personal Data Protection, which promotes collaboration and harmonization of cyber laws.

1.4.9. Enforcement Agencies

Uganda Police Force: The police have a specialized Cybercrime Unit within the Criminal Investigations Directorate (CID). This unit investigates cybercrime incidents, gathers digital evidence, and collaborates with other law enforcement agencies.

National Computer Emergency Response Team (CERT**)**: CERT Uganda is responsible for monitoring and responding to cybersecurity incidents. It also provides guidance on cybersecurity best practices and facilitates information sharing among stakeholders.

Judiciary: The judiciary plays a critical role in adjudicating cybercrime cases, interpreting laws, and ensuring fair trials.

1.4.10. Prosecution Process

Reporting and Investigation: Victims of cybercrime can report incidents to law enforcement, where the Cybercrime Unit will investigate the allegations. This involves gathering digital evidence, interviewing witnesses, and collaborating with technology companies as needed.

Legal Proceedings: Once sufficient evidence is collected, the case is forwarded to the Directorate of Public Prosecutions (DPP) for legal action. The DPP decides whether to prosecute based on the evidence available.

Trial: Cases are brought before the courts, where the prosecution must prove the defendant's guilt beyond a reasonable doubt. Legal frameworks allow for various forms of evidence, including digital forensics.

1.4.11. Recent Developments

Capacity Building: There are ongoing initiatives aimed at improving the skills of law enforcement and judicial personnel in handling cybercrime cases. Training programs often involve collaboration with international organizations and experts.

Public Awareness Campaigns: The government and NGOs are working to raise awareness about cyber threats, safe online practices, and the legal implications of cybercrimes.

Collaboration with Private Sector: Increasing partnerships between the government and private sector entities, especially telecommunications companies, help to enhance cybersecurity measures and improve incident response.

Regional Cooperation: Uganda is actively engaging with other East African nations to strengthen regional cybersecurity frameworks and facilitate cooperation in investigating and prosecuting cybercrimes The prosecution of cybercrimes in Uganda has gained prominence as the country experiences rapid digitalization and increased internet penetration. The government has recognized the importance of addressing cyber threats to protect individuals, businesses, and national security. Here's an in-depth look at the various aspects of how Uganda approaches the prosecution of cybercrimes:

1.5. CONCLUSION

As it is elaborated above, cybercrime target governments and individuals as well. The motive might be political, criminal or social. Politically, we have witnessed elections in powerful States being influenced from thousands of kilometers through internet. This is because cybercrime, like air pollution, knows of no borders and crosses from one country to another without visas. Criminals are accessing Credit Cards and Bank Accounts of unsuspecting people and emptying them. At personal level, couples are harassing each other through the internet, notwithstanding their technological backwardness, East African States, while having diverse national frameworks, have not developed a strong joint regional legal framework to address cybercrime.

CHAPTER2: CHALLENGES IN THE PROSECUTION OF CYBERCRIMES IN THE EAC

The prosecution of cybercrime in East African Community is crucial difficult due to different reasons like lack of harmonized legal framework, absence of uniformity in the definition of cybercrime which lead to different interpretation of cyber offences, lack of harmonized legal system, the jurisdictional challenges and institutional challenges which comprised by inadequate legal experts in cybercrime's, capacity limitation for both investigators and judges, and lack of special unit designed to deal with only cybercrime.[62]

2.1. LACK OF HARMONIZED LEGAL FRAMEWORKS

According to the lack harmonized legal frameworks with in members of East African Community, it produces catastrophic challenge which hinders the effective combating cybercrime within region, this challenge led to inconsistencies in how cybercrimes are defined, investigated, and prosecuted across borders, hampering regional cooperation and enforcement efforts.[63]

2.1.1. The lack of uniformity in definition of cybercrime

The absence of harmonized definition of cybercrime within member state of East African Community led to interpretation conflicts and challenge in prosecuting cross-borderer cybercrimes, as an example the legal framework of Kenya provide a definition encompassing wide range of cyber offences,[64] Uganda's legal framework provide more limited scope,[65] due to this uniformity, there is jurisdictional conflicts and legal ambiguities in the prosecution of cybercrime in East African Community as criminal act in some state and other did not legalize it. As its impacts, offenders for those cybercrime benefit those gaps seeking refuge in the countries with less strength definition or enforcement mechanisms which affects the combating cybercrime effectively in the region.[66]

Moreover, the lack of standardized definition of cyber offences hinders the international co-operations and mutual legal assistance which is important in prosecuting cybercrimes with

[62] Mwiburi A J, Preventing and Combating Cybercrime in East Africa, Lessons from Europe's Cybercrime Frameworks, The German national library (2018) P 48-53.

[63] Mwiburi A J, supra note 1, p 50.

[64] Republic of Kenya, The computer misuse and cybercrime Acts, (2018) OG supplement nº. 60, Acts nº 5.

[65] The computer Misuse acts, Acts Supplement to The Uganda Gazette No. 10 Volume CIV dated 14th February, 2011. Printed by UPPC, Entebbe, by Order of the Government

[66] UNCTAD, Harmonizing cyber laws and Regulations: The experience of East African Community, United Nations (2012) P8.

transnational element, the different legal framework within EAC has an impacts in adoption of dual criminality, a principle which is necessary for extradition and evidence transition in cross border cases, this challenge not only hinder the process of collecting and presenting evidence across jurisdiction but also challenge joint investigations and prosecution among member state.[67]

2.1.2. The absence of uniform procedure laws within EAC

In East African Community, there are different Procedural laws governing cybercrime investigations, for some member countries like Kenya have specific provisions for digital evidence collection and preservation in their Evidence Act[68] and other like Uganda, Burundi and South Sudan has no clear guidelines and regulations and rely on general evidence rules which is unclear guidelines that cannot address the challenges of digital evidence, this differences produce challenges in admissibility of evidence in cross-border cases and may result in criminals exploiting these gaps to evade justice, the absence of common procedure laws within EAC affect effectiveness of criminal justice from gathering evidence to the court proceedings. As consequences, evidence that may be admissible in one state may not be admissible in other which may result in the dismissal of cases of cybercrime according to the procedure rather than the merits of the case.[69]

Furthermore, the absence of uniform procedure laws within the EAC produce challenges relating with jurisdictional issues and enforcement of court judgement with in region. The transnational element of cybercrime requires cooperation between law enforcement agencies and judiciaries of different EAC member states but due to lack of uniformity in procedural laws hinder this cooperation and become difficult to determine which country has jurisdiction over a particular cybercrime case and how to resolve conflicts when many countries are involved.[70]

2.1.3. The lack of harmonized legal system

The East African Community (EAC) is characterized by a different legal system within member states which apply different legal system, this lack of uniformity in legal system produce different challenges in the effectiveness of prosecution of cybercrime within the region, Currently, Uganda, Kenya, and Tanzania primarily follow the common law system which is

[67] UNCTAD, supra note 1, p 8.

[68] The Data Protection Act, Supra note 1.

[69] One trust data guidance, Comparing Privacy laws, GDPR vs Kenya data protection Acts, (2019)p 20. Available at https://www.dataguidance.com/sites/default/files/gdpr_v._kenya.pdf accessed on 06 July 2024.

[70] Walumoli B B, A critical analysis of the challenge facing counter cybercrime in 21st century in Africa: A focused comparison of Kenya and Rwanda, University of Nairobi (2019), p 22-30.

derived from their colonial master British, it is contrary with Rwanda and Burundi where they apply legal civil law systems rooted its source Belgium as their colonial, but in this era Rwanda evolving by mixing both legal system, this fundamental difference in legal systems creates substantial obstacles in harmonizing approaches to cybercrime prosecution across the EAC.[71]

2.2. JURISDICTIONAL ISSUES

The jurisdictional challenge led to different challenge in the investigation, prosecution and adjudication of cybercrime in East African Community, specifically for those with cross-border element, the cyberspace is unlimited which conflicts with traditional principle of territorial jurisdiction and produce difficulties for law enforcement and judicial systems.[72]As an example, when cybercriminals in Kenya attacks a server in South Sudan and affecting victims in Bujumbura, it will be difficult to determine which state has primary obligation to prosecute because this scenario is not predetermined in all countries of EAC.[73] Even if this principle of territorial jurisdiction applied in criminal matters, it is not easy in cyber related crime, the principle of extradition process in East African community is also complicated in cybercrime because EAC laws do not specifically determine the procedure for extradition for cybercrime with transnational element, it is found as gap which led to complex in prosecuting cybercriminals who work internationally but reside in one state member of EAC.[74]

2.3. Institutional challenges

The institutional challenge is one of challenging issue in combating cybercrime is the fact that it is borderless and cross territorial in nature, and its impacts are much wider than those of traditional crimes, it means that while the legal and institutional frameworks are grounded on real geographical locations, cybercrimes are not affected by physical boundaries as such. For that matter, cybercrime poses threats not only to the confidentiality, integrity or availability of computer systems, but also to the security of critical infrastructure. It is for this reason that a call for the fight against this contemporary form of criminality inevitably necessitates employing

[71] Review Process of the Eastern Africa Law Review, A Journal of Law and Development, University of Dar es Salaam School of Law, University of Dar es Salaam, vol 42, issue no 2, (2017) p 80.

[72]Dragoijlovic J, Jrisdiction for criminal offence of cybercrime: international and national standards, University of the Academy of Economics in Novi Sad, Serbia (2023) p64-67.

[74] Kaniki A O J, supra note 1, P 27.

individual and the collective initiatives and efforts among States at regional and inter-regional levels to combat the same.[75]

2.3.1. The lack of specialized cybercrime units in EAC

The specialized unit for cybercrime within East African Community is an important because they will help in the effective investigation of complex cybercrimes that require specific technical expertise, in EAC state members lacks necessary technical understanding to effectively adjudicate cybercrime cases.[76] This is evident in the limited provisions for continuous judicial training on cybercrime matters in most EAC countries' legal frameworks, some state do not explicitly provide for special training for judges, investigators, and prosecutors in cybercrime matters which lead to misinterpretation or misapplication of cybercrime laws.[77]

Insufficient forensic capabilities pose another significant institutional challenge, the lack adequate forensic facilities and expertise to handle digital evidence, this deficiency can lead to challenges in evidence collection, preservation, and presentation in court, potentially compromising cybercrime prosecutions, the absence of comprehensive data protection laws in some EAC, this lack of uniformity in data protection frameworks can hinder cross-border investigations and information sharing among EAC law enforcement agencies, institutional challenges also arise from the limited capacity of prosecution services to handle cybercrime cases, this shortage of expertise can lead to ineffective prosecution of complex cybercrime cases, potentially resulting in low conviction rates.[78]

2.3.2. Inadequate technical and legal expertise

Inadequate technical and legal expertise presents a significant challenge for law enforcement agencies and judicial systems in the EAC when investigating, prosecuting, and adjudicating cybercrimes, particularly those with cross-border elements; this gap in specialized knowledge hampers the effective application of cybercrime laws and the handling of complex digital evidence.[79] Due to increase cybercrime often outpaces the technical expertise of law enforcement

[75] Johnson D R & David G P, Law and borders-The rise of law in cyberspace, Stanford law Review,Temple University Beasley school of law, vol 48 (1996) p 1367.

[76] Johnson D R et al , supra note 1, p 1340.

[77]Council of Europe, Global action on cybercrime extended, Principle of judicial training in cybercrime and electronc evidence, (2017) p 2-6.

[78] Rakha A N, Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations, Mexican Law Review, (2024) p 18.

[79] Ejayi E F G, Challenges in enforcing cyber-crimes laws and policy, Journal of internet and information systems, Kenyata University School of law, Vol6, issue no 1 (2016) p 4-7.

agencies in the EAC, there must be team of expert in EAC with skills in cyber laws, this gap can lead to ineffective evidence collection and analysis, potentially compromising prosecutions and legal expertise specific to cybercrime is often lacking in the prosecution services across the EAC.[80]This absence of specialized prosecutors can result in inadequate case preparation and presentation, potentially leading to acquittals in complex cybercrime cases, the judiciary in many EAC countries lacks sufficient training in cybercrime-related legal issues and digital evidence handling; this knowledge gap can lead to misinterpretation of technical evidence and misapplication of cybercrime laws, potentially resulting in flawed judgments.[81]

The challenge of inadequate expertise is further compounded by the cross-border nature of many cybercrimes. While the EAC has the East African Community Protocol on Peace and Security, which provides for cooperation in combating transnational crimes, the implementation is hindered by varying levels of technical and legal expertise across member states. This disparity can impede effective cross-border investigations and prosecutions; The lack of expertise also extends to digital forensics capabilities. This deficiency can lead to challenges in preserving the integrity of digital evidence and presenting it effectively in court, potentially undermining cybercrime prosecutions.[82]

2.3.3. Unable resources for law enforcement agencies

The capacity limitations of law enforcement agencies and unable resources is also major challenge in the prosecution of cybercrime in the East African Community, Capacity limitations of law enforcement agencies produce challenge in investigating, prosecuting, and adjudicating cybercrimes within the EAC, specifically for those with transnational elements, these limitations encompass inadequate resources basing on money , insufficient training and motivations and a lack of specialized units dedicated to combating cybercrime, the shortage of adequate technological resources further exacerbates the capacity limitations, this resource gap can lead to ineffective evidence collection and analysis, potentially compromising prosecutions.[83]

[80] Ejayi E F G, supra note 1, p 5.

[81] Ejayi E F G, supra note 2, p 8.

[82] Owino V, cybercriminals on the internet target East African Firms most, The East African, available at https://www.theeastafrican.co.ke/tea/business/cybercriminals-on-the-continent-target-east-african-firms-most-3951524 accessed on 07 July 2024.

[83] Moloney C J et al Assesing law enforcements cybercrime capacity and capability, (2022) available at https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability- accessed on 07 July 2024.

Training deficiencies also contribute significantly to capacity limitations which hinder the prosecution of cybercrime within EAC, without continuous and up-to-date training for law enforcement officers, the effective prosecution of cybercrime will remain challenging, and the rapidly evolving nature of cybercrime necessitates ongoing training programs, which are often lacking due to resource constraints.[84] Forensic capabilities, crucial for cybercrime investigations, are often limited within EAC law enforcement agencies, this deficiency can lead to challenges in preserving the integrity of digital evidence and presenting it effectively in court, the capacity to handle large volumes of data in cybercrime investigations is another significant limitation, the law enforcement agencies lack the necessary data analysis tools and skills to process the vast amounts of digital information often involved in cybercrime cases. This can result in prolonged investigations and potential loss of crucial evidence.[85]

2.4. Identification of case related to the subject matter

Below there is analysis for the Case NO: RP/ECON 00002/2020/TGI/GSBO, ON 30/06/2021, before Gasabo intermediate court relating with cybercrime and the key challenges do the court face due to lack of harmonized cybercrime laws in East African Community.

2.4.1. Parties to the case

Prosecution: Represented by SEJEMBA Ismaël and NTEZIRYIMANA Sylvain, 22 Accused individuals, primarily from Kenya and Rwanda, Civil Damages Claimant: EQUITY BANK represented by Me MUHIGANWA Damas[86]

2.4.2. Alleged offences

Unauthorized access to a computer or computer system data, access to data with intent to commit an offense, unauthorized modification of computer or computer system data, theft, formation of or joining a criminal association[87]

2.4.3. Summary of the case

Equity Bank in Rwanda received information about a group of criminals, including Dedan MUCHOKI MURIUKI, who entered Rwanda intending to steal money from the bank. The group's modus operandi involved using customers' ATM cards to access and steal funds. Equity Bank informed the Rwanda Investigation Bureau (RIB), which initiated an investigation. The

[84] Moloney C J et al supra note 1.

[85] Owino V, supra note 1.

[86] Prosecution Vs Dedan Muchoki Muriuk and others, CASE NO: RP/ECON 00002/2020/TGI/GSBO, before Gasabo intermediate court on 30/06/2021, p 1-3.

[87] Prosecution Vs Dedan Muchoki Muriuk and others, p 2

criminal group approached a Rwandan citizen, KIIZA, who cooperated with authorities to gather evidence. The group used an application called Em Cert ID app to manipulate bank accounts. They were arrested at Equity Bank's REMERA branch after attempting to steal money from 23 bank accounts, successfully manipulating 8 accounts to steal 2,944,283 Rwandan Francs.[88]

2.4.4. Key Defendants and Their Roles

The following are defendants with their responsibilities.[89]

A. Dedan MUCHOKI MURIUKI: Alleged leader of the group
B. Samuel WACHIRA NYUNGUTO: Supervisor in the criminal operation
C. KINYUA Erickson MACHARIA: Responsible for withdrawing and collecting money
D. KAGABO Robert: Provided his account for transferring stolen money
E. Seth KABERA: Provided his account for the operation
F. Godfrey GACHIRI GITHINJI: Part of the arrested group
G. Eric Dickson NJANGI MUTEGI: Member of the criminal association
H. Reuben KIRONGOTHI MWANGI: Facilitated movements and kept items for the group
I. Damaris NJERI KAMAU: Provided bank accounts to facilitate the crime
J. KAYITANA Julias: Provided his account for fraudulent transfers
K. Several other individuals who provided their bank accounts or assisted in various capacities

2.4.5. Court Proceedings

The court examined evidence presented by the prosecution, including witness testimonies, confessions, digital forensic reports, and physical evidence. Many defendants pleaded not guilty, claiming lack of intent or knowledge of the criminal activities. The court analyzed each defendant's role in the criminal operation, considering their actions, intent, and the evidence presented against them.[90]

[88] Prosecution Vs Dedan Muchoki Muriuk and others, para 1- 2
[89] Prosecution Vs Dedan Muchoki Muriuk and others, p 1-3
[90] Prosecution Vs Dedan Muchoki Muriuk and others, para 3-53, p 4-14

2.4.6. Court's Findings

The court found all 22 defendants guilty of the five charged offenses. The judgment was based on various pieces of evidence, including:[91]

A. Confessions and testimonies

B. Digital forensic evidence

C. Physical evidence (e.g., confiscated items)

D. Bank transaction records

E. Witness statements

2.4.7. Sentencing

Each of the 22 defendants was sentenced to 8 years of imprisonment. The court applied the maximum sentence as provided for in Articles 61 and 62 of Law no 68/2018 of 30/08/2018, considering the crimes as an ideal concurrence of offenses.[92]

2.4.8. The court's decision on damages

The following are decision taken by court for damages.[93]

A. Ordered all convicts to jointly repay the stolen amount of 2,994,783 Rwandan Francs

B. Granted 50,000,000 Rwandan Francs for moral damages

C. Awarded 100,000 Rwandan Francs for expert consultation fees

D. Ordered repayment of travel and maintenance expenses for experts

E. Awarded 1,000,000 Rwandan Francs for legal fees

2.4.9. Challenges Faced by the Court due to Lack of Harmonized Cybercrime Laws in the East African Community

Jurisdictional Issues: The case involved criminals from multiple East African countries, primarily Kenya and Rwanda. The lack of harmonized laws made it challenging to determine the extent of jurisdiction and how to handle cross-border aspects of the crime.

Differences in Legal Definitions: Cybercrime definitions and classifications may vary between East African countries. This could create difficulties in prosecuting offenders for specific cyber offenses that might be defined differently or not exist in other jurisdictions.

[91] Prosecution Vs Dedan Muchoki Muriuk and others, para 5-54, p5-15

[92] Prosecution Vs Dedan Muchoki Muriuk and others, para 53-55, p 13-14

[93] Prosecution Vs Dedan Muchoki Muriuk and others, para 56-58, p 14-15.

Evidentiary Challenges: The admissibility and weight of digital evidence may differ across jurisdictions. Without harmonized laws, the court may have faced challenges in determining how to treat certain types of digital evidence or forensic reports.

Sentencing Disparities: The lack of uniform sentencing guidelines for cybercrime across the East African Community may have made it difficult for the court to ensure that the sentences were consistent with regional standards and practices.

International Cooperation: The absence of harmonized laws could have hindered efficient cooperation between law enforcement agencies and courts in different East African countries, potentially impacting the investigation and prosecution process.

Extradition Issues: For defendants who were not present in Rwanda, the lack of harmonized cybercrime laws might have complicated extradition processes, as the principle of dual criminality might not be easily established.

Technological Expertise: The court may have faced challenges in accessing appropriate technological expertise to understand and evaluate complex cybercrime evidence, as standards for such expertise might vary across the region.

Procedural Differences: Variations in criminal procedures across East African countries could have created challenges in handling certain aspects of the case, especially those involving cross-border elements.

Addressing Novel Cyber Threats: The rapid evolution of cyber threats might outpace legislation in individual countries. A lack of harmonized, up-to-date laws could have made it difficult for the court to address newer forms of cybercrime effectively.

Balancing Rights and Law Enforcement: Without a unified approach, the court may have struggled to balance individual rights (such as privacy and data protection) with the needs of law enforcement in cybercrime cases.

2.5. Conclusion

It is emphasized that the seriousness and threats posed by cybercrime and Considering the anonymity of cyberspace, it may, in fact, be one of the most dangerous criminal threats we will ever face in East African Community as we are not safe from what is happening in the world, in terms of technological developments and also criminal threats and trends. The East African region covers a land area of 1.82 million square kilometers and it is home to 149.7 million people,[94] this population as a whole can, therefore, be contemplated as comprising potential victims of cyber criminality. Under the East African Community portfolio, the region has been forging cooperation among Member States in addressing common problems facing its inhabitants. In briefly, the effective combating cybercrime in East African Community are challenged by different factors as it mentioned above, like lack of harmonized legal framework.

[94] The East African Community Secretariat, p. 15.

CHAPTER3: MECHANISMS FOR EFFECTIVE CYBERCRIME PROSECUTION

According to the mentioned challenges, the prosecution of cybercrime in EAC is not well effective which hinder the development and infringe rights of individuals and business companies, there must be establishment of effective mechanisms and solutions with purpose of combating cybercrime within EAC region. The following are different proposed mechanisms to be adopted with in EAC as the way of achieving effective prosecuting cybercrime.

3.1. Harmonization of cybercrime laws in the EAC

The harmonization of cybercrime laws across the East African Community (EAC) is crucial for a cohesive legal framework to combat transnational cybercrime, which often transcends geographical boundaries. Standardizing definitions and digital evidence across member states can create more resilient cases, maintaining integrity across borders;[95] harmonization creates a unified front against cybercrime, fostering a shared understanding of cybercrime and prosecution, this is crucial in regions with technological disparities and legal sophistication, harmonized laws provide a clear framework, streamlining the prosecution process and preventing cybercriminals from evading justice, the harmonization of legal frameworks in the East African Community ensures the admissibility of digital evidence across borders, enhancing its probative value in cross-border cases due to its volatile nature.[96]

The harmonization of cybercrime laws in the EAC enhances cross-border cooperation, facilitating smoother collaboration between law enforcement agencies and judiciaries, and improving the speed and efficiency of cybercrime investigations, harmonized laws support Mutual Legal Assistance Treaties (MLATs) by creating a common legal language, reducing bureaucratic hurdles and facilitating faster information exchange, this efficiency is crucial in cybercrime where rapid acquisition of digital evidence is crucial for successful prosecution.[98]Harmonized laws enable joint investigation teams (JITs) across the EAC to work efficiently, effectively tracking cybercriminals and gathering admissible evidence, especially in complex cases involving sophisticated networks, the harmonized laws in EAC countries

[95] Jerome U O, The African Union Convention on Cybersecurity: A regional response towards cyber stability? Masaryk University Journal of Law and Technology Vol 12, issue no 2, (2017) p 100.

[96] James N O, Meeting the challenge of cyber threats in emerging electronic transaction technologies in Kenyan Banking sector, PHD Theses, University of Nairobi (2015) p 45-54

[98] Jerome U O, supra note 1, p 120

encourage the creation of shared databases and information-sharing platforms, ensuring data protection and enhancing prosecutors' ability to build comprehensive cases.[99]

The harmonization of cybercrime laws in the EAC promotes capacity building and specialization in cybercrime prosecution, addressing technical complexities.[100] This approach fosters specialized prosecutors with deep understanding of legal and technical aspects of digital crimes, harmonized legal frameworks in the EAC facilitate knowledge sharing and best practices across borders, particularly in the dynamic field of cybercrime, and this knowledge sharing enables prosecutors to learn from each other's successes and challenges, enabling effective strategies for tackling new cyber threats. Harmonized laws enable standardized certification programs for cybercrime prosecutors across the EAC, enhancing competence and mobility of expertise, thereby enhancing the quality of prosecutions and promoting regional cooperation.[101]

The EAC's harmonization of cybercrime laws enhances private sector engagement and international cooperation, promoting effective prosecution and facilitating cooperation in investigations, especially with private companies owning critical infrastructure and data, the ITU report on cybersecurity in Africa highlights harmonized laws, enabling multinational corporations and internet service providers to develop regional policies for data retention and reporting, reducing compliance burdens, and promoting investment in robust cybersecurity measures.[102] Harmonized laws improve EAC's cybersecurity engagement through public-private partnerships, attracting private sector investment in shared initiatives like training programs and threat intelligence platforms, the EAC's unified legal approach to cybercrime enhances international cooperation, providing resources, expertise, and support for law enforcement agencies.[103] This aligns with international standards like the Budapest Convention on Cybercrime, facilitating smoother global investigations; the EAC's harmonized laws strengthen its role in international cybercrime policy discussions, allowing it to shape global strategies that consider the unique challenges and perspectives of the region.[104]

[99] United Nation, Harmonizing cyber laws and regulations : the experience of East African Community, UNCTAD, (2012) P5-10

[100] East African Communications Organization, 'Cybersecurity Policy Guidelines for the EAC Region, (2022)

[101] Beer D J et al Framework for assessing technology hubs in Africa, , journal of intellectual property and entertainment law, vol 6, issue no 2, (2017) p270.

[102] Mwibur A J, preventing and combating cybercrime in East Africa, Lesson from European cybercrime frameworks, The Faculty of Law and Economics of the University of Bayreuth, (2018) p 205-213

[103] Mwibur A J, Supra note 1, p 205-2013

[104] Mwibur A J, Supra note 2, 154-189

3.1.1. The importance of harmonizing cybercrime laws in the EAC to protect the rights and interests of individuals and businesses

It is critical to harmonize cybercrime regulations within the East African Community (EAC) in order to promote efficient cross-border collaboration in cybercrime investigations, the international scope of cybercrime presents formidable obstacles for law enforcement organizations that are limited by national borders, different national laws do not impede the seamless collaboration, evidence sharing, and joint operations between these agencies where there are uniform legal frameworks in place, given that hackers frequently take advantage of jurisdictional variations to avoid punishment, this coordination is crucial.[105] The EAC is implementing a unified methodology to standardize digital evidence collection, preservation, and admissibility in courts; this helps close legal gaps and promotes cross-border knowledge exchange. Harmonized regulations also facilitate collaboration between cybercrime units and local centers of excellence; this strategy expedites investigations and sends a strong deterrent message to potential cybercriminals.[106]

Harmonized cybercrime laws in the EAC region provide legal certainty and predictability, benefiting individuals and businesses by ensuring a clear understanding of cybercrime across member states, this reduces the risk of non-compliance and ensures uniform application of legal rights and obligations, this clarity is crucial in the era of remote work and digital nomadism. Harmonized regulations also lower compliance costs and legal concerns, improving operational efficiency and encouraging businesses to invest in digital infrastructure, a uniform legal framework for cybercrime in the EAC would improve security, attract foreign investment, and foster trust in digital systems.[107] Harmonized laws would safeguard individual privacy and data rights, promoting equal protection across borders, this would also address emerging privacy challenges, such as biometric data protection and AI-driven processing, fostering digital economy growth and cross-border data flows.[108]

The East African Community (EAC) is proposing harmonized laws to streamline operations, promote investment, and level the playing field for local startups and SMEs, while also boosting

[105] Briyan Sang YK & Ivan s, a comparative review of cybercrime law in Kenya: Juxtaposing national legislation with international treaty standards, The commonwealth cybercrime journal, (2018) p 69

[106] Kshetri, N. Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, vol 22, issue no 2 (2019) p 77–81

[107] Kshetri, N supra note 1, p 56

[108] Kshetri, N supra note 2, p 60

consumer confidence in digital sectors, the harmonization of cybercrime laws in the EAC region improves cybersecurity and resilience by establishing common standards and protocols. This standardization facilitates efficient cyber threat sharing, regional intelligence platforms, and a robust cybersecurity infrastructure, particularly in Africa, to address evolving threats and resource constraints.[109]

3.2. Strengthening of existing legal frameworks

Strengthening EAC's legal frameworks is crucial for comprehensive coverage of cyber offenses and effective prosecution. Current laws were enacted before sophisticated threats, leaving gaps in addressing modern digital crimes. Regular updates ensure prosecutors have relevant legal provisions to tackle complex offenses like cryptojacking and deepfakes. Regular adaptation also helps prevent cybercriminals from falling through legal loopholes.[110] Strengthening legal frameworks in the East African Community (EAC) is crucial for effective cybercrime prosecution; these frameworks improve procedural laws and evidentiary standards, providing clear guidelines on digital evidence admissibility and weight. They also enable information sharing and mutual legal assistance among member states.[111] The EACO emphasizes the importance of strengthened legal frameworks in justifying investment in technological resources and skills development for cybercrime prosecution. This enhancement boosts the effectiveness of cybercrime prosecutions across the EAC.[112]The African Union Commission emphasizes the importance of strengthening the legal frameworks in the EAC for international cooperation and effective cybercrime prosecution, the updated laws align with international standards and conventions, enhancing the region's ability to handle complex cases and promoting harmonization of cybercrime laws. This is crucial for effective information sharing and joint operations among African nations.[113]

[109] East African Community adopts framework for cyberlaws to foster regional trade, investment, UNCTAD/PRESS/IN/2010/023 available at https://unctad.org/press-material/east-african-community-adopts-framework-cyberlaws-foster-regional-trade-investment accessed on 31 July 2024.

[110] Council of Europe, the state of cybercrime in Africa- an overview, available at https://rm.coe.int/16806b8a79 accessed on 30 July 2024.

[111] Farai T, Emerging cyber security threats: a comparative study of Kenya and Zimbabwe, University of Nairobi, Cyber security threats, Phd Theses, (2020) p 14-20

[112] Farai T, supra note 1, p 11

[113] Cerezo I A et al the international cooperation to fights transnational cybercrime, Computer science department, University of Malaga Spain, (2007) p 70.

3.3. Training and specialization of law enforcement and judicial personnel

Training and specialization of law enforcement and judicial personnel in Eastern Africa (EAC) is crucial for effective cybercrime prosecution. Specialized programs equip personnel with skills to collect, analyze, and present digital evidence. The United Nations Office on Drugs and Crime emphasizes continuous training to keep pace with evolving threats and digital forensic techniques. Hands-on, practical training simulates real-world cybercrime scenarios, enhancing the EAC's capacity to investigate, prosecute, and adjudicate complex cases.[114]

Specialized training for law enforcement and judicial personnel in the East African Community (EAC) improves evidence handling and case preparation for successful cybercrime prosecution. This enhances understanding of digital evidence, ensuring admissibility and weight in court proceedings. The EACO emphasizes standardized protocols for digital evidence collection and preservation. Prosecutors' training links digital evidence to cyber offenses, securing convictions in complex cases. Cross-disciplinary training combines legal knowledge with technical skills.[115]

Specialized training programs for law enforcement and judicial personnel enhance international cooperation, particularly in prosecuting cybercrime in the EAC. These programs improve collaboration, tracking cybercriminals across borders, and gathering evidence. They also foster a common understanding of cybercrime issues, enabling smoother international collaboration and handling international requests for evidence and extradition.[116]The training and specialization of law enforcement and judicial personnel in cybercrime expertise and specialized units enhances the EAC's capacity to prosecute complex cyber offenses. These units, staffed by experts in digital forensics and investigation, handle complex cases more efficiently than general crime units. Specialized training also fosters the establishment of dedicated cybercrime courts, ensuring informed judgments and robust cybercrime jurisprudence.[117]

3.4. Establishment of dedicated cybercrime units

The East African Community (EAC) has established dedicated cybercrime units, enhancing the fight against digital crime. These multidisciplinary teams, with expertise in cybersecurity, digital forensics, and legal frameworks, offer a sophisticated, targeted approach to investigating and

[114] Mwaita P & Owor M, workshop report on effective cybercrime legislation in Eastern Africa Dar es Salaam, Tanzania, (2013) p 25.

[115] Stardust M et al, The law society of Kenya Journal, council members of the law society of Kenya (2022-2024) Vol 19 (2023)p 100.

[116] Mwiburi A J, supra note 2, p 60.

[117] The world Bank, Combating Cybercrime, tools and capacity building for emerging economics, United Nations, (2017) p 300.

prosecuting cyber offenses. Their focus on cyber-related crimes allows them to stay ahead of technological advancements and criminal methodologies. The specialized units in East Africa's cybercrime prosecution focus on developing protocols for digital evidence collection, preservation, and analysis, ensuring court admissibility and resulting in higher conviction rates, serving as a deterrent to potential cybercriminals and strengthening the rule of law in cyberspace.[118] Dedicated cybercrime units are essential for international cooperation and combating transnational cybercrimes. They act as centralized points of contact for cross-border investigations, streamlining the process and facilitating efficient information sharing. They coordinate joint operations, bridging operational and legal gaps between jurisdictions. These units can navigate the complex landscape of international cybercrime, coordinate raids, share threat intelligence, and develop new investigative techniques. They also harmonize legal approaches to cybercrime, making cross-border prosecution more feasible. This enhances the EAC's collective ability to close loopholes in cybercrime prosecution.[119]

The establishment of dedicated cybercrime units in the Eastern Caribbean (ECA) is crucial for capacity building and specialized expertise in the region's fight against cybercrime. These units act as knowledge hubs, continuously refining and disseminating best practices in cybercrime investigation and prosecution. They provide comprehensive training programs for various stakeholders, covering topics such as digital literacy, cybersecurity awareness, and prosecuting complex cases. They also collaborate with academic institutions and international organizations to develop new tools and regional guidelines for handling digital evidence. This ongoing process ensures the EAC's approach to cybercrime remains dynamic and adaptive.[120]

Cybercrime units in the European Cyberspace (EAC) are crucial in shaping and harmonizing cybercrime legislation across member states. They provide valuable feedback to policymakers on the effectiveness of current legislation and the need for legal reforms. They identify gaps in existing laws, highlight outdated definitions, and propose amendments to better reflect the realities of cybercrime in the digital age. They also advocate for harmonization of cybercrime laws, creating consistent legal standards and definitions, and facilitating cross-border cooperation

[118] Muendo M, what’s been done to fights against cybercrime in East Africa, the conversation (2019) available at https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240 accessed on 30 July 2024

[119] Owino V, Cyber-criminals on the continent target East African Firms most, (2022) available at https://www.theeastafrican.co.ke/tea/business/cybercriminals-on-the-continent-target-east-african-firms-most-3951524 accessed on 30 July 2024

[120] Odhiambo E, Transnational Cooperation in Cybercrime Prosecution: Lessons for the EAC, University of Nairobi PhD thesis, (2023) P 178-185.

in cybercrime cases. They also engage in comparative legal analysis and advocate for international conventions on cybercrime.[121]

3.5. Information sharing and joint investigations

Information sharing is vital for the East African Community (EAC) to improve cybercrime prosecution, by exchanging intelligence, threat data, and best practices, member states can detect, investigate, and prosecute cybercriminal activities; this collaborative approach prevents the spread of attacks and facilitates coordinated responses. Sharing legal strategies, case studies, and prosecutorial techniques also enhances the effectiveness of cybercrime investigations, especially in countries with varying expertise.[122] Joint investigations among EAC countries are crucial for tackling cross-border cybercrimes. They allow for efficient sharing of resources, expertise, and jurisdictional authority, enabling comprehensive cases against criminals operating across multiple countries. These investigations also help overcome legal hurdles, ensuring admissible evidence in all relevant jurisdictions, enhancing the chances of successful prosecution.[123]

Advanced technological solutions in the EAC are enhancing information sharing and joint investigations for cybercrime prosecution, these include secure communication platforms, shared databases, and AI-powered analytics tools, these tools enable efficient collaboration and rapid exchange of digital evidence, ensuring the integrity and traceability of evidence. By leveraging these tools, the EAC can create a more agile and effective cybercrime prosecution framework. The EAC needs to establish a harmonized legal and policy framework to maximize information sharing and joint investigations in cybercrime prosecution. This includes developing standardized protocols, ensuring data protection laws, and creating clear guidelines for joint operations. This harmonization addresses legal and jurisdictional challenges, sends a strong deterrent message, and facilitates cooperation with international partners.[124]

3.6. Collaboration with international organizations

The East African Community (EAC) is leveraging international organizations like INTERPOL, UNODC, and ITU to enhance its capacity to prosecute cybercrimes. These organizations provide specialized knowledge and technical assistance, enabling the EAC to tackle the complex nature

[121] Natia M, The international response against cyber-crime, international journal of cybersecurity studies, (2024)

[122] Macdonald A, How successful has the international community been in its response to the Rise of cybercrime?, an examination of the conditions that have allowed cybercrime to thrive and the mixed efforts of the international community to control it, Staffordshire University (2017) p 42-68.

[123] Macdonald A, supra note 1, p 45

[124] Macdonald A, supra note 2, p 50

of cybercrime. These partnerships involve capacity-building programs, training local law enforcement on the latest techniques and legal frameworks, thereby enhancing the EAC's cybercrime prosecution capabilities.[125] International organizations like EUROPOL facilitate cross-border cooperation and information sharing for prosecuting cybercrimes. EAC countries benefit from these networks for real-time intelligence sharing, accessing critical information about emerging threats and ongoing investigations. These collaborations enable EAC countries to effectively track and apprehend cybercriminals, even when operating from outside the region, and enhance the likelihood of successful prosecutions.[126]

Collaboration with international organizations like the Council of Europe and UNODC helps harmonize legal frameworks and develop comprehensive cybercrime legislation within the EAC. These organizations provide model laws and guidelines, ensuring the region's legal framework is robust and aligned with international standards, this harmonization facilitates cross-border investigations and prosecutions, and enhances the EAC's ability to engage in mutual legal assistance and extradition processes with global cybercriminals.[127] International organizations like the World Bank and the African Development Bank support the development of technological infrastructure and analytical capabilities for effective cybercrime prosecution in the EAC. These organizations help establish Computer Emergency Response Teams (CERTs) and enhance cybersecurity capabilities, enabling efficient detection, tracking, and analysis of cyber threats. Collaborations with these organizations can help overcome resource limitations and establish a more sophisticated cybercrime prosecution infrastructure.[128]

3.7. Implementation of Data Protection and Privacy Frameworks

The East African Community's data protection and privacy frameworks are crucial in combating cybercrime by establishing clear guidelines for handling and transmitting personal and sensitive data. These laws enforce strict security measures, compel organizations to invest in cybersecurity infrastructure, and facilitate cross-border data transfers, thereby safeguarding individual privacy

[125] I-EAC Project, Combating terrorism and transnational organized crime in East African region, INTERPOL available at https://www.interpol.int/How-we-work/Border-management/I-EAC-Project accessed on 30 July 2024

[126] I-EAC Project, supra note 1

[127] Commission on the crime prevention and criminal justice, How can the commission on crime prevention and criminal justice contribute to the accelerated implementation of the 2030 agenda, in particular goal 16? Contribution by member state and stackeholders, Contributions by the Commission to the work of the Economic and Social Council, in line with General Assembly resolutions 75/290 A and 75/290 B, including follow-up to and review and implementation of the 2030 Agenda for Sustainable Development

[128] Callejas J F et al, United Nations, Cybersecurity in the United Nations system organisations, Report of the Joint Inspection Unit, Geneva (2021) p 83-92

rights, data protection and privacy frameworks enhance cybercrime detection and reporting by defining data breaches and mandating timely reporting, this transparency increases visibility, enabling law enforcement to develop effective strategies. Implementing comprehensive data protection regimes fosters a culture of cybersecurity awareness and compliance, crucial for proactive prevention.[129]

The EAC's adoption of data protection and privacy frameworks can enhance international cooperation in cybercrime prosecution, harmonized data protection standards, aligned with best practices, facilitate smoother collaboration with global partners. These frameworks provide a common language for handling digital evidence, making joint investigations easier. This strengthens the EAC's position in the global cybercrime fight.[130]

3.8. Establishment of specialized cybercrime courts

The East African Community is establishing specialized cybercrime courts to improve the prosecution of digital crimes, these courts, staffed by judges with specialized training in cybercrime and digital forensics, can handle technical complexities, ensuring accurate interpretation of digital evidence and more informed judgments.[131]Specialized cybercrime courts can significantly enhance the speed and efficiency of cybercrime prosecutions in the EAC, by handling cybercrime cases consistently; these courts establish clear legal precedents and interpretations of cybercrime laws, providing clarity in a rapidly evolving area of law. [132] This is especially important in the context of emerging cyber threats. Specialized courts can adapt quickly to technological changes and ensure the legal framework remains relevant and effective. They can also contribute to harmonization of regional cybercrime legislation, facilitating more effective cross-border prosecutions and sending a clear deterrent message to potential cybercriminals.[133]

3.9. Creation of regional cybercrime coordination centers

The establishment of Regional Cybercrime Coordination Centers (RCCCs) in the East African Community represents a significant leap forward in the fight against cybercrime. These centers serve as focal points for coordinating cybercrime investigations, intelligence sharing, and

[129] Makulilo A B, privacy and data protection in Africa: international data privacy law, vol2, issue 2, (2012) p 163-167

[130] Serianu, Africa cyber security report 2019, (2020) p 42

[131] Kshetri N, Cybercrime and cybersecurity in Africa, journal of global information technology management, vol 22, issue no 2, (2019) p 77-79

[132] Cassim F, addressing the spectre of cybercrime: A critical analysis of the adequacy of legal framework for cybercrime in South Africa, de jure law journal, vol 53, issue no 3, (2020) p 358-372

[133] Cassim F, supra note 1, p 366

strategic planning across member states.[134] 'Regional coordination is crucial in addressing the transnational nature of cybercrime, which often exploits jurisdictional differences to evade prosecution'. RCCCs can facilitate rapid information exchange, enabling law enforcement agencies to respond swiftly to emerging cyber threats. They can also standardize cybercrime reporting mechanisms across the region, creating a comprehensive picture of the cybercrime landscape in East Africa. This centralized approach to data collection and analysis can reveal patterns and trends in cybercriminal activities, informing more effective prevention and prosecution strategies. Moreover, as highlighted in the African Union's Cybersecurity Expert Group report, such centers can 'foster the development of shared technical infrastructure and tools, maximizing resource utilization and enhancing the overall cybercrime fighting capability of the region.[135]

Regional Cybercrime Coordination Centers (RCCCs) are being established to improve the European Union's (EAC) international cooperation and align with global best practices in cybercrime prosecution. These centers can streamline cross-border investigations, provide legal assistance, and enhance the region's voice in international cybercrime fighting efforts. They also aid in harmonizing cybercrime laws and procedures, enhancing the EAC's overall cybersecurity posture.[136]

3.10. Enhancing digital forensics capabilities

The East African Community (EAC) is investing in digital forensics capabilities to improve its ability to investigate and prosecute cybercrimes. This includes the collection, preservation, and analysis of electronic evidence. By investing in advanced tools, EAC member states can trace digital footprints, reconstruct incidents, and link cybercriminals to their actions more effectively. The African Union (EAC) is enhancing its digital forensics capabilities to build capacity and expertise in cybercrime investigation units.[137] This involves providing specialized training in digital forensics techniques, enhancing the credibility of digital evidence, and enabling the EAC to participate more effectively in international cybercrime investigations, the African Union's

[134] Kahihu P, cybersecurity and cybercrime in East Africa: A cross=country analysis, journal of cyber policy, vol 4, issue no 2 (2020) p 175-188

[135] International Telecommunication Union, Guide to developing a National cybersecutity started (ITU) (2018) p 89

[136] Olayemi O J, Combating cybercrime in Sub-Saharian Africa: Adisclosuer in Law, policy and practice, journal of law, technology and trust, vol13, issue no 1 (2022) p 1-15

[137] Munyua A, cybersecurity and digital Resilience in East Africa, journal of cyber policy, Vol 6, issue no 1, (2020) p 9-22

cybersecurity guidelines emphasize the importance of enhanced digital forensics capabilities in global efforts against cybercrime.[138]

The EAC region can significantly reduce cybercrime by enhancing digital forensics capabilities. Advanced techniques can identify patterns and trends in cyber-attacks, enabling law enforcement to develop effective preventive strategies, this knowledge can deter potential cybercriminals and support the development of robust cybersecurity policies and standards, by leveraging these capabilities, the EAC can create a more hostile environment for cybercriminals, ultimately reducing incidents.[139]

3.11. Development of Cybercrime Reporting Mechanisms and Platforms

The East African Community (EAC) needs robust cybercrime reporting mechanisms and platforms to enhance prosecution and improve law enforcement responses, these systems provide structured and accessible means for individuals, businesses, and organizations to report cyber incidents, increasing visibility and enabling more effective responses, efficient reporting reduces time between cybercrime occurrence and detection, and standardizes reporting across the region, revealing cross-border patterns and supporting coordinated responses.[140]

Cybercrime reporting mechanisms and platforms are essential for building public trust and engagement in cybersecurity efforts. EAC countries can demonstrate commitment by providing accessible channels, enhancing public education on best practices, and gathering intelligence on emerging threats, these mechanisms can create a dynamic cybersecurity ecosystem, leveraging citizens' and businesses' collective vigilance, and facilitate collaboration between public and private sectors in combating cybercrime.[141]Cybercrime reporting mechanisms and platforms in the East African Community help in effective resource allocation and policy-making in cybercrime prosecution, they provide accurate data on cybercrime, enabling informed decisions about resource allocation, training needs, and legislative priorities, these platforms can be

[138] Oludayo O & Olopade O, digital forensics and the cybercrime ecosystem in Nigeria: challenges and prospects, international journal of cyber criminology, vol 8, issue no 2, (2021) p 172-185

[139] Victor R K & Ray I, a generic digital forensic investigation framewok for internet of things (IoT), IEEE international conference on future internet of things and cloud (2016) p 356-360

[140] Ndiaye A, cybercrime in West Africa: Pourign old wine into new bottles? Journal of cyber policy, vol 7, issue no 1, (2020) p 94-105

[141] Muthuri R et al, cybercrime land scape and legal framework in Kenya, international journal of cyber criminology, vol 15, issue no 3 (2021) p 174-189

integrated with data analytics tools to identify trends and emerging threats, enabling proactive responses and evidence-based policy-making.[142]

[142] Kaboi S & Waema T, cybersecurity capacity building in developing countries: A case study of Kenya, international journal of informational security and cybercrime, vol 4, issue no 2, (2019) p 31-40

4. GENERAL CONCLUSIONS AND RECOMMENDATIONS

This study is composed by three chapters, general introduction is composed by elaborating the background cybercrime in EAC, the problem statement, research questions, research methodology, interest of study and research objective, after that there is chapter one which comprise the theoretical framework of child marriage by elaborating definition of key terms, like cybercrime, digital evidence, data protection, cybersecurity, dark web, hacking, phishing, cyber terrorism and others, it discusses the concept of cybercrime in details and analyses mental and material element of cybercrime, it presents different theories relating with legal and jurisdictional system basing on transnational legal theory, deterrence theory, legal pluralism, universal jurisdiction and complementarity, chapter one is ended by short history of EAC.

Chapter two is composed by elaborating the problem of this study in details by elaborating the challenges in the prosecution of cybercrime in EAC, the study provide numerous challenges like lack of harmonized legal framework, lack of uniform procedure laws, jurisdiction issues, institutional challenges, lack of specialized cybercrime unit in EAC, lack of enough resources and others, before concluding this chapter, the study analyses case adjudicated by intermediate court of Gasabo which is relating with cybercrime and provide challenges court faced due to transnational character of cybercrime. The last chapter is three which is made of mechanisms and solutions for effective cybercrime prosecutions, where this study propose the harmonization of cybercrime laws in EAC, strengthening of existing legal framework, training and specialization of law enforcement and judicial personal, establishment of dedicated cybercrime unit, information sharing and joint investigations and collaboration with international organizations.

Conclusively, as emphasized in this study, combating cybercrimes and enhancing cyber-security is no longer a national matter but a global concern. Therefore, countries need to combine efforts in addressing the issue. This is true for EAC Member States since it is better for the interests of the Community that there is minimal criminal activity. The EAC is also bound to provide services to its citizens and in the course provide a safe environment at both the regional and international levels. This study has revealed that EAC Member States depend on each other in the fight against cybercrimes. It is until such efforts are realized and the cyber laws are harmonized when the war towards cybercriminals may be said to be won. As revealed from the study, currently there are challenges when trying to address cybercrimes involving other regional states due to the fact that these crimes are defined and punished differently in the EAC States. What is a cybercrime in Kenya may not be a crime in Rwanda or Burundi.

Even though individual EAC Member States are making efforts in addressing cybercrimes at their national level more needs to be done towards establishing effective cooperation channels among each other. The institutions tasked with the research, investigation and prosecution of these offences should work with greater synergy. The study has identified a number of initiatives made and areas of convergence and divergence, challenges and proposed some direction in addressing these. This study recommends to the EAC legislative body to implement those mechanisms and solutions proposed under chapter three of this study by emphasizing on the harmonizing cybercrime laws, strengthening of existing legal framework, training and specialization of law enforcement and judicial personal, establishment of dedicated cybercrime unit, information sharing and joint investigations and collaboration with international organizations. This will enable the effective prosecution of cybercrime in EAC and reduce the number of those criminals who escape justice due to hide themselves in the nations which doesn’t regulate cybercrime effectively.

2. BIBLIOGRAPHY

2.1. Legislations

2.1.1. International legislation

1. United Nations Conference on Trade and Development, East African Community, Draft EAC Legal Framework for Cyber Laws (2008)
2. United Nations Conference on Trade and Development, East African Community, Draft EAC Legal Framework for Cyber Laws (2008)
3. East African Communications Organization, 'Cybersecurity Policy Guidelines for the EAC Region, (2022)
4. Rome Statute of the International Criminal Court July 17, 1998, 2187 U.N.T.S. 90

2.1.2. National legislation

1. Republic of Kenya, The computer misuse and cybercrime Acts, (2018) OG supplement nº. 60, Acts nº 5.
2. The computer Misuse acts, Acts Supplement to The Uganda Gazette No. 10 Volume CIV dated 14th February, 2011. Printed by UPPC, Entebbe, by Order of the Government
3. One trust data guidance, Comparing Privacy laws, GDPR vs Kenya data protection Acts, (2019)
4. Law No. 60/2018 of 22/08/2018 on the Prevention and Punishment of Cybercrime

2.1.3. Case laws

1. United States v. Ali, 718 F.3d 929, 935-38 (D.C. Cir. 2013)
2. United States v. Yousef, 327 F.3d 56, 104 (2d Cir. 2003)
3. Prosecution Vs Dedan Muchoki Muriuk and others, CASE NO: RP/ECON 00002/2020/TGI/GSBO, before Gasabo intermediate

2.2. Law reports

1. The Hon. Chief Justice of Uganda, Mr. Justice Benjamin Odoki, *Justice for Everyone: a Myth or Reality? From the Ugandan perspective, Conference Report*
2. African Union Commission, *2019 African Regional Integration Report, Towards an Integrated Prosperous and Peaceful Africa*
3. UNCTAD *Harmonizing Cyber Laws and Regulations: The Experience of the East African Community, United Nations,* New York, (2013)

4. UNCTAD, *Harmonizing cyber laws and Regulations: The experience of East African Community, United Nations* (2012)
5. Council of Europe, *Global action on cybercrime extended, Principle of judicial training in cybercrime and electronc evidence*, (2017)
6. United Nation, *Harmonizing cyber laws and regulations : the experience of East African Community,* UNCTAD, (2012)
7. The world Bank, *Combating Cybercrime, tools and capacity building for emerging economics, United Nations*, (2017)
8. I-EAC *Project, Combating terrorism and transnational organized crime in East African region,* INTERPOL
9. *Commission on the crime prevention and criminal justice, How can the commission on crime prevention and criminal justice contribute to the accelerated implementation of the 2030 agenda, in particular goal 16? Contribution by member state and stackeholders, Contributions by the Commission to the work of the Economic and Social Council, in line with General Assembly resolutions 75/290 A and 75/290 B, including follow-up to and review and implementation of the 2030 Agenda for Sustainable Development*
10. ITU, *Understanding cybercrime:Phenomenon, challenges and legal response, ITU Telecommunications development sector,* (2012)
11. Serianu, *Africa cyber security report 2019*, (2020)

2.3. Law review

1. Rakha A N, *Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations, Mexican Law Review*, (2024)
2. Hunton, Paul, *The growing phenomenon of crime and the internet: A cybercrime execution and analysis model, Computer Law and Security Review, 29*, (2009)

2.3. Books

1. Prof. Chaubey R K, *An Introduction to Cybercrime and Cyber Law, Kamal Law House* (2012).
2. Walumoli B B, *A critical analysis of the challenge facing counter cybercrime in 21st century in Africa: A focused comparison of Kenya and Rwanda,* University of Nairobi (2019)

3. Gorman L, *Maclean D Media and Society in Twentieth Century, Blackwell publishing*, 2003.
4. Mwiburi A J, *Preventing and Combating Cybercrime in East Africa, Lessons from Europe's Cybercrime Frameworks, The German national library* (2018)
5. Dragoijlovic J, *Jrisdiction for criminal offence of cybercrime: international and national standards, University of the Academy of Economics in Novi Sad, Serbia* (2023)
6. Owino V, *cybercriminals on the internet target East African Firms most, The East African,*
7. Moloney C J *et al Assesing law enforcements cybercrime capacity and capability,* (2022)
8. Ibraham D *et al, The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press*, (2001).
9. Marco, G. *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (Ed)(2012)
10. Majamba H L *et al Harmonization of cybercrime legal frameworks within East African Community*, University of Dar-es-Salaam School of Law
11. Athina, K 'Introduction: *New Media and the Reconfiguration of Power in Global politics' in Karatzogianni Athina (Ed), Cyber Conflict and Global Politics, Routledge*, ., (2008)
12. Fafinski, et al *Mapping and Measuring Cybercrime', OII Forum, Paper* No 18, (2010)
13. Achieng, R. *Expert Meeting on Cyberlaws and Regulations for Enhancing E-Commerce: Including Case Studies and Lessons Learned*, (2015),
14. Makulilo, A.B, *Protection of Personal Data in sub-Saharan Africa, PhD Thesis, University of Bremen, Germany*, 2012
15. Kiongo, G. G. *Harmonization of Cyber Crime Laws in the East African Community: A Comparative Analysis* (Doctoral dissertation, University of Nairobi) (2020).
16. Okello, J. O. *Cyber Crime Prosecution in the East African Community: Towards a Harmonized Legal Framework* (Doctoral dissertation, Makerere University). (2019).
17. Zaidy A A, *Digital crime and our society, Academia Letters* (2022),
18. Maujili, *jurisdictional challenges in fighting cybercrimes: any panacea from international law?* (2015)

19. Schjolberg S & Ghernaouti-Hélie S, *A Global Protocol on Cybersecurity and Cybercrime, Cybercrime data*(2009)
20. Dentzel Z, *How the internet has changed everyday life, OPENMIND BBVA*,
21. Doyle S, *Cybercrime and violent crime are converging: here how to deal with it, World Economic Forum*, (2023),
22. United Nations, *Comprehensive study on cybercrime, United Nation Office on Drug and crime,* (2013)
23. Johnson B, *Do criminal law deters crime? Deterrence theory in criminal justice policy: A primier, MN House Research*, (2019)
24. James N O, *Meeting the challenge of cyber threats in emerging electronic transaction technologies in Kenyan Banking sector, PHD Theses*, University of Nairobi (2015)
25. Mwibur A J, *preventing and combating cybercrime in East Africa, Lesson from European cybercrime frameworks, The Faculty of Law and Economics of the University of Bayreuth,* (2018)
26. Farai T, *Emerging cyber security threats: a comparative study of Kenya and Zimbabwe, University of Nairobi, Cyber security threats, Phd Theses*, (2020)
27. Cerezo I A et al *the international cooperation to fights transnational cybercrime, Computer science department*, University of Malaga Spain, (2007)
28. Mwaita P & Owor M, *workshop report on effective cybercrime legislation in Eastern Africa Dar es Salaam, Tanzania*, (2013
29. Muendo M, *what's been done to fights against cybercrime in East Africa, the conversation* (2019)
30. Owino V, *Cyber-criminals on the continent target East African Firms most, (2022)*
31. *Odhiambo E, Transnational Cooperation in Cybercrime Prosecution: Lessons for the EAC, University of Nairobi PhD thesis*, (2023)
32. Macdonald A, *How successful has the international community been in its response to the Rise of cybercrime?, an examination of the conditions that have allowed cybercrime to thrive and the mixed efforts of the international community to control it, Staffordshire University* (2017)
33. Natia M, *The international response against cyber-crime, international journal of cybersecurity studies*, (2024)

34. Callejas J F et al, *United Nations, Cybersecurity in the United Nations system organisations, Report of the Joint Inspection Unit*, Geneva (2021)
35. ITU, *Understanding cybercrime: Phenomenon, challenges and legal response, ITU Telecommunications development sector*, (2012)
36. Stevenson R L B, '*Plugging the "Phishing" Hole: Legislation versus Technology', 5 Duke Law & Technology Review*, (2005)
37. Higgins R, *problems and process: International law and how we use it, oxford public international law*, (1995)
38. Hunton, Paul, *'The growing phenomenon of crime and the internet: A cybercrime execution and analysis model'*, *Computer Law and Security Review*, 29, (2009)
39. International Telecommunication Union, *Guide to developing a National cybersecutity started* (ITU) (2018)
40. Victor R K & Ray I, *a generic digital forensic investigation framewok for internet of things (IoT), IEEE international conference on future internet of things and cloud* (2016)

2.4. Journals

1. Mwingira, A. C., & Kanyarus, J. B *Challenges in the Prosecution of Cyber Crimes in the East African Community. Journal of African Law*, (2021). vol 65, issue no 2, p 215-238.
2. Chimilila C *et al* Trade Facilitation in EAC Customs Union: Its Achievement and Implementation in Tanzania, Journal Of Economics and Sustainable Development, Vol. 5, issue No.25 (2014)
3. Nyamache, E. O. The Role of the East African Court of Justice in Enhancing Regional Cooperation on Cyber Crime Prosecution. East African Law Review, (2022). Vol 44 issue no 2.
4. Beer D J et al *Framework for assessing technology hubs in Africa, , journal of intellectual property and entertainment law*, vol 6, issue no 2, (2017)
5. McGrath, J.E. *Methodology Matters: Doing Research in the Behavioural and Social Sciences,* in Baecker, R. M.et al. (1995). *Readings in Human-Computer Interaction: Toward the Year 2000*, Morgan Kaufmann Publishers, p.154, as quoted in Makulilo, A, B., note 124. See also, Singhal, A. K. and Malik, I, *Doctrinal and Social Legal Methods: Merits and Demerits, Educational Research Journal*, 2012, Vol.2, No.7

6. Anabo, I. F, *Prosecuting Cyber Crimes in the East African Community: Challenges and Prospects. East African Journal of Peace & Human Rights*, (2019), vol 25 issue no 1.
7. DR. ADEL AZZAM S H, *Jurisdiction in Cybercrimes: A Comparative Study, Journal of Law, Policy and Globalization*, vol 22, (2014
8. Prof. Sharma P, *A Review of International Legal Framework to Combat Cybercrime, nternational Journal of Advanced Research in Computer Science*, Vol 8, issue No. 5, (2017),
9. Cassim F, *Protecting personal information in the era of theft: just how safe is our personal information from identity thieves?* Vol 18, issue no 2, (2015),
10. Alexandra P G, *Transnational cyber offences, overcoming jurisdictional challenges, the yale journal of international law,* vol 43, (2018)
11. Merry S E, *Legal pluralism, Law and society Review*, vol 22, issue no 5, (1988)
12. *Review Process of the Eastern Africa Law Review, A Journal of Law and Development, University of Dar es Salaam School of Law*, University of Dar es Salaam, vol 42, issue no 2, (2017)
13. Kaniki A O J, *International Dipolmatic Review Journal, examination of security challenge in the East African Community (EAC) region* , vol 1, issue no 2, (2022)
14. Johnson D R & David G P, *Law and borders-The rise of law in cyberspace, Stanford law Review,Temple University Beasley school of law*, vol 48 (1996)
15. Ejayi E F G, *Challenges in enforcing cyber-crimes laws and policy, Journal of internet and information systems, Kenyata University School of law*, Vol6, issue no 1 (2016)
16. Jerome U O, *The African Union Convention on Cybersecurity: A regional response towards cyber stability? Masaryk University Journal of Law and Technology* Vol 12, issue no 2, (2017)
17. Stardust M et al, *The law society of Kenya Journal, council members of the law society of Kenya* (2022-2024) Vol 19 (2023)
18. Kyoung S M et al, *an International comparative study on cyber security strategy, an international jpournal of security and its application*, vol 9, issue no 2 (2015)

19. Prof. Sharma P, *A Review of International Legal Framework to Combat Cybercrime, nternational Journal of Advanced Research in Computer Science*, Vol 8, issue No. 5, (2017),

20. Snail S, *cybercrime in South Africa, hacking, cracking and other unlawful online activities, journal of information, law & technology*, vol 1, (2009)

21. Hoofnagle C J, *Identity theft: Making the kown unknowns known 2007 Harvard Journal of Law & Techinology*, vol 21, (2007)

22. Ashiru A, *identifying phishing as form of cyber-crime in Nigeria, Department of Public and Private Law, Lagos State University, Lagos-Badagry Expressway* vol 12, issue no 2(2021)

23. Kyoung S M et al, *an International comparative study on cyber security strategy, an international journal of security and its application*, vol 9, issue no 2 (2015)

24. Briyan Sang YK & Ivan s, *a comparative review of cybercrime law in Kenya: Juxtaposing national legislation with international treaty standards, The commonwealth cybercrime journal,* (2018)

25. Kshetri, N. *Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management*, vol 22, issue no 2 (2019)

26. Makulilo A B, *privacy and data protection in Africa: international data privacy law*, vol2, issue 2, (2012)

27. Kshetri N, *Cybercrime and cybersecurity in Africa, journal of global information technology management,* vol 22, issue no 2, (2019)

28. Cassim F, *addressing the spectre of cybercrime: A critical analysis of the adequacy of legal framework for cybercrime in South Africa, de jure law journal*, vol 53, issue no 3, (2020

29. Kahihu P, *cybersecurity and cybercrime in East Africa: A cross=country analysis, journal of cyber policy,* vol 4, issue no 2 (2020)

30. Olayemi O J, *Combating cybercrime in Sub-Saharian Africa: Adisclosuer in Law, policy and practice, journal of law, technology and trust*, vol13, issue no 1 (2022)

31. Oludayo O & Olopade O*, digital forensics and the cybercrime ecosystem in Nigeria: challenges and prospects, international journal of cyber criminology*, vol 8, issue no 2, (2021)

32. Munyua A, *cybersecurity and digital Resilience in East Africa, journal of cyber policy*, Vol 6, issue no 1, (2020)
33. Ndiaye A, cybercrime in West Africa: Pourign old wine into new bottles? Journal of cyber policy, vol 7, issue no 1, (2020)
34. Muthuri R et al, *cybercrime land scape and legal framework in Kenya, international journal of cyber criminology,* vol 15, issue no 3 (2021)
35. Kaboi S & Waema T, *cybersecurity capacity building in developing countries: A case study of Kenya, international journal of informational security and cybercrime*, vol 4, issue no 2, (2019)

2.4. Electronic sources

1. Anon,*Cybercrime-prosecutionguidance*,https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance
2. *East African Community, 'History of the EAC'* https://www.eac.int/eac-history
3. *East African Community, 'History of the EAC'* https://www.eac.int/eac-history
4. *East African Community, 'EAC Mission and Vision'* https://www.eac.int/about-eac
5. *Council of Europe, the state of cybercrime in Africa- an overview*, available at https://rm.coe.int/16806b8a79 accessed on 30 July 2024.