International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Mutual Legal Assistance in Combating Cybercrimes in the East African Community

Essau Abraham Sengo

Research and Teaching Assistant, College of Business Education (CBE)

ABSTRACT

This paper is devoted to exposing the challenges facing the East African Community in fighting computer crimes. Several comparisons were made where Kenya, Uganda, Burundi, Rwanda, and Tanzania were used as focal points in examining the effort and mutual assistance in fighting cybercrimes. It was, however, revealed that computer crime has increased, and so have the computer cyber challenges. Looking into the bigger picture of cyber offences around the world, Africa, especially the East Africa Community, is not immune to cyberattacks, and henceforth, there is a dire need for a common understanding of such mischief at the global and regional levels.

This thesis depicts the solution to these challenges, including global legislation and the mutual assistance of all states. Although currently there is no global legislation to counter transnational cyber offences, East Africa, on the other hand, has shown a way through its EAC Treaty, which is not even effective in deploring mutual and joint efforts in addressing the problem of cybercrimes in the whole of East Africa. This thesis has given credit to Rwanda as a member of the EAC, which has good and comprehensive legislation dealing with computer crimes and is the only single-country effort in the absence of a majority. Likewise, this thesis has expounded on the existing gap in Chapter 4, which has addressed computer crime in the EAC, and recommendations were made, especially to learn from other countries that have succeeded in fighting computer crimes, including Rwanda. The study deployed qualitative research methods as an alternative to gathering information. The reason was that qualitative research improves a substantial part of the law, which could result in achieving the broader goal of the study.

Key words: Cybercrimes, Mutual Legal Assistance, Cybersecurity, East African Community

1. Introduction

Mutual legal assistance in criminal matters means a process in which State seeks and provides assistance in gathering evidence for use in criminal cases from other States. The mutual legal assistance may be requested for purpose of taking evidence or statements from persons, effecting service of judicial documents, executing searches, seizures and freezing, examining objects and sites, providing information, evidentiary items and expert evaluations, providing originals or certified copies of relevant documents and records including government, bank, financial, corporate or business records, identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes,

facilitating the voluntary appearance of persons in the requesting State party and any other type of assistance that is not contrary to the domestic law of the requested State party.[1]

In this paper, the reference to criminal matters or cases is limited to the assistance rendered in relation to cybercrimes. It is worth noting that a country cannot independently and effectively fight against cybercrimes on its own. The nature of cybercrimes demands cooperation from all States in combating them. Cybercrimes are subtle in that the location of the offenders is hardly known and obscure.[2] The need to protect the population of the East African Community (EAC) against the cybercrimes cannot be overstated. Currently there are seven Member States of the EAC that is the United Republic of Tanzania, Uganda, Kenya, Rwanda, Democratic Republic of Congo, South Sudan as well as Burundi. The collaborative efforts amongst countries constituting the EAC are necessary in combating cybercrimes.

To shed light on this critical issue and reinforce the collaborative efforts, this study examined and assessed the existing legal framework governing mutual legal assistance in combating cybercrimes in the EAC. Through collaborative efforts exhibited by the shared framework on mutual legal assistance, traditional barriers to an effective collaboration among the States can be avoided. On that basis, the possibility of the requesting State[3] to prosecute cybercriminals whose evidence is located outside the country is guaranteed and, in that way, cybercriminals are insecure to work within the country located in the community where there is an effective collaboration governed by the robust legal mutual assistance framework. The traditional tool of mutual legal assistance in criminal matters has been letters rogatory - a formal request from the judicial authority of one State to a judicial authority of another State, where the requested judicial authority is asked to perform one or more specified actions, usually collecting evidence and interviewing witnesses, on behalf of the requesting judicial authority.[4] These requests are conventionally transmitted through diplomatic channels.[5] The processes are usually lengthy, costly, and time-consuming and, nowadays in the digital era, they may prove impractical.

Despite the swift move the world is undertaking to respond to the challenges of cybercrimes through the existence of clear provisions of the law providing for the need to establish effective legal and institutional framework for fighting cybercrimes, it is evident that the EAC Member States have not established any legal instrument to facilitate mutual legal assistance in waging war against cybercrimes.

Efforts to harmonize cyber laws as a significant step in fostering mutual legal assistance among the EAC Member States (Tanzania, Kenya, and Uganda) began in 2006 with support from the United National Conference on Trade and Development (UNCTAD).[6] A special Task Force was formed and charged with the task of conducting a comprehensive research, review and examination of the reality and

[1] United Nations Office on Drugs and Crimes, Manual on Mutual Legal Assistance and Extradition, United Nations Office, Vienna, 2012, p.19 and www.unodc.org.

[2] Mwiburi, A.J and Majamba, H. I, "Overview and Methodological Approach in Harmonizing Cybercrimes Law in East Africa" in Mwiburi, A.J and Majamba, H. I, Harmonization of Cybercrimes Legal Frameworks within the East African Community, University of Dar es Salaam School of Law, Dar es Salaam, 2020, p.1.

[3] According to the Law on Mutual Legal Assistance in Criminal Matters (Official Gazette of Montenegro, No. 04/08 dated 17.01.2008), requesting State means foreign State the competent judicial authority of which sent the letter rogatory for international legal assistance; and requested State means the foreign State to which the letter rogatory for international legal assistance is sent. Available at https://www.vertic.org/media/National%20Legislation/Montenegro/ME_Law_Mutual_Legal_Assistance.pdf.

[4] Computer Crime and Cybercrime: Alternative SADC Model Law on Computer Crime and Cybercrime, 2022, 1050, Connecticut Ave. N.W., Suite 45., Washington, D.C. 20036.

[5] Idem.

[6] Mwiburi, A.J and Majamba, H. I, "Overview and Methodological Approach in Harmonizing Cybercrimes Law in East Africa" op. cit., p.3.

challenges facing the Member States.[7] It was required to come up with measures that will not only address problems common to all but that would also address challenges brought due to the differences in their legal systems.[8] Among the major findings of this Task Force was that the laws in the Member States forming the then EAC were not harmonized and provide divergences in national approaches to cybercrimes.[9]

2. The Legal Problem

Member States of the EAC have been maintaining scattered and distinct laws on mutual legal assistance in cybercrimes. The presence of distinct laws unique to the Member States is an indication that there is no cooperation. This is the reality although the essence of forming the community was to enhance collaboration in all important affairs among its members. The uncollaborated efforts in enacting robust laws on mutual legal assistance exhibited in the EAC is more devastating in relation to cybercrimes than traditional criminal activities committed in the borders of the community. Criminals consider uncollaborated efforts to end crimes as an opportunity to expand their criminal operations.

Cybercriminals take advantage of weaknesses in cybercrime legislation and the nascent systems of law enforcement leading to a proliferation of illicit activities.[10] Being borderless and transnational in nature, cybercrimes require collective efforts to investigate, prosecute, and punish its offenders.[11] Despite the need for the collective framework on mutual legal assistance among the EAC Member States, EAC does not have a single binding framework on the mutual legal assistance with regard to general crimes and particularly in relation to cybercrimes. Importantly, under Article 28(2) of the African Union Convention on Cyber Security and Personal Data Protection (the **Malabo Convention**), the State Parties that do not have agreements on mutual assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis. Furthermore, under Article 28(4) of the Malabo Convention, the State Parties are required to make use of existing means for international cooperation with a view to responding to cyber threats, improving cyber security and stimulating dialogue between stakeholders. These means may be international, intergovernmental or regional, or based on private and public partnership. Interestingly, it is only Rwanda which has ratified the Malabo Convention making it another hurdle for all EAC Member States to have a common goal in ending cybercrimes in the sub-region.[12]

Given the above, the study examined and assessed the existing legal framework governing mutual legal assistance in combating cybercrimes in the EAC. The study indicates areas that the EAC should focus on for purposes of ensuring that cybercriminals are not afforded with the opportunity to further their criminal activities with impunity. Although the establishment of computer and cybercrime mutual legal framework for addressing criminal matters and extradition is essential across the regions on the account

[7] Ibiden.
[8] Idem.
[9] Id.
[10] Mwaita P and Owor M, *Workshop Report on Effective Cybercrime Legislation in Eastern Africa*, Dar es Salaam, Tanzania, 22 August 22-24, 2013, p.1.
[11] Ibiden.
[12] List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection: Https://Au.Int/En/Treaties/African-Union-Convention-Cyber-Security-And-Personal-Data-Protection Accessed On 17 October 2023.

that several legal issues occur in the course of dealing with cybercrime cases,[13] and despite the fact that Article 124(5) of the EAC Treaty requires Member States to strive to cooperate in handling cross border crimes and provide mutual assistance in criminal matters,[14] such a workable framework is yet to be developed to address cybercrimes. The lack of this significant framework has led to an increasing rate of cybercrimes. The EAC remains a haven for cyber criminals. It is against this backdrop that the study examined the legal framework on mutual legal assistance framework to address cybercrimes.

3. Literature Review

This part presents some of the studies exploring mutual legal assistance, and cybercrimes. Books and other writings from different writers are reviewed. The review aims at exploring and putting forth what other authors have written in relation to the proposed study. Each literature has been reviewed on two perspectives. First it explores what makes it relevant to the study; and second on what makes it different from this study.

Muendo[15] asserts that the digital space has many positive attributes but the threat of cybercrime and insecurity is evident. Uganda lost 42 million shillings to cybercrime in 2017. In 2018, Rwanda lost 6 billion francs. In Kenya, between April and June 2019 alone, the country experienced 26.6 million cyber threats. Across the region, with the increase of digital banking, financial institutions have become targets.[16] These institutions are attractive to cyber criminals because they hold the biggest cash reserves. Africa's digital infrastructure is ill-equipped to manage the continent's growing cyber-security risk.

The statistics as put forth by the author help to appreciate the implications of the lower collective responses against the challenges posed by the cyber environment. [17] However, contrary to what the study proposes to cover, the author has limited the information on the effects of cybercrimes to only three States (Uganda, Kenya, and Rwanda).

Mwiburi and Majamba[18] argue that cybercrime challenges have international dimension, limiting efforts in combating such crimes at the national and regional levels. Cybercriminals tend to operate from countries with weak regulations and attacking even the strong cyber regulated ones. Collective effort amongst countries is a critical tool to fighting against cybercrimes which know no borders. The authors hold the view that there is a need for the global and regional harmonisation of legal efforts in addressing cyber-issues, especially cyber-security. To ensure regional integration and welfare of citizens, the EAC needs to address cyber-security concerns at the national level and address harmonisation of cyber laws to tackle the international aspects of these challenges.[19] In essence, the differences in mutual legal assistance provisions make Member States unable to cooperate and assist each other in investigating, collecting and even sharing important information required in prosecuting cybercriminals, hence, leaving them unprosecuted and unpunished. Despite the significance contribution of this writing there is

[13] United Nations Office on Drugs and Crimes, *Manual on Mutual Legal Assistance and Extradition*, United Nations Office, Vienna, 2012.
[14] The Treaty Establishing the East African Community, 1999, Arusha. EAC: 2002 xiv, 111: 230mm (EAC Publication, No.1).
[15] Mercy Muendo, **What's been done to Fight Cybercrime in East Africa, 2019,** https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240**.**
[16] Ibiden
[17] **Idem.**
[18] Mwiburi, A.J and Majamba, H. I, "Overview and Methodological Approach in Harmonizing Cybercrimes Law in East Africa" in Mwiburi, A.J and Majamba, H. I, Harmonization of Cybercrimes Legal Frameworks within the East African Community, University of Dar es Salaam School of Law, Dar es Salaam, 2020.
[19] Mwaita Patrick and Owor Maureen, op. cit.., p.2.

a need to trace the developments that have happened since 2020 when the authors came up with such findings and corresponding recommendations.

Rees[20] points to the challenges brought by the principle of dual criminality which is traditionally necessary for two countries to cooperate on a particular criminal matter. In his opinion, countries must agree on what to criminalize in order to overcome the challenges posed by the dual criminality divide. Rees suggests countries to amend their laws in order to foster cooperation amongst themselves. Whereas the author focuses on forging countries to cooperate for purposes of stimulating mutual legal assistance in relation to cybercrime investigations, this study is specific to the collaborative efforts among the Member States constituting the EAC.

Verdelho[21] puts forth that due to the expansion of communication networks, particularly the internet, it is impossible for any country in the world to act alone against cybercrimes. As the use of Internet increases, it gives more possibilities to criminals, and provide them with new opportunities to commit crimes remotely. Verdelho adds that the only adequate approach to address the borderless nature of global networks is a common approach, where domestic efforts are complemented by specific forms and channels of international co-operation that can face the issue of crime being facilitated globally, with potential consequences in any part of the world.[22] The difference the study makes from this writing is that it is not confined to the Members of the European Union. It covers the Eastern part of Africa, particularly in relation to the Member States of the EAC.

De Busser[23] opines that the traditional mechanism of mutual legal assistance is losing ground quickly because of its slow and cumbersome way of workingWith surveys showing that it takes authorities an average of ten months to react to a request for mutual legal assistance in some cases, no reaction is received at all by the individual requesting authority, as well as the European Union institutions, have sought faster alternatives. Ten months is slow in any criminal investigation even in a domestic setting, but it is unworkably slow when the evidence is in digital rather than in physical or intangible form.[24] According to the author, the rapid increase of digital evidence for all types of criminal offences - not just computer-related offences - emphasizes the slowness and general inadequacy of the traditional cooperation system. Digital evidence introduces not only a volatile type of information that can be highly relevant to criminal investigations, but also presents a world of territorially organized national criminal laws with the inherently exterritorial world of digital data.[25] Combining the two seems to push States towards a move away from mutual legal assistance. Recent efforts have been directed at solving the problem of slow cooperation but seem to avoid the question of human rights protection which is the basic thing to consider.[26] Conversely, this study explores how the East African Community is deployed as an opportunity in relation to legal mutual assistance and fight against cybercrimes.

Bailey[27] is of the view that the ends of criminal justice, such as sound conviction of the right person for the right reasons, and the protection of fundamental rights, such as the freedom from arbitrary detention

[20]Rees A., International Cooperation in Cybercrime Investigations, Computer Crime & Intellectual Property Section Criminal Division, U.S. Department of Justice. OAS Regional Cyber Crime Workshop, April 2007.
[21] Verdelho P., the Effectiveness of International Co-operation against Cybercrime: Examples of Good Practice, Economic Crime Division Directorate General of Human Rights and Legal Affairs Strasbourg, France, 2008, p.4.
[22] Ibiden
[23] De Busser, E.D, The Digital Unfitness of Mutual Legal Assistance, *Security and Human Rights*, 2017, Vol.28, pp.161-179.
[24] Ibiden
[25] ibid
[26] Ibid
[27] Bailey, E.C, *Counterterrorism Law and Practice in the East African Community*, Brill Nijhoff, Boston, 2019, p. 165.

and torture, should be mutually compatible goals. The EAC Member States should consider the UN Model Treaty on Extradition, as well as the subsequent experience of the Economic Community of West African States (ECOWAS) in adopting a mutual legal assistance treaty.[28]Although the author could not focus directly on cybercrimes, the views expressed with regards to the need for the EAC Member States to develop their own mutual legal assistance treaty equip the study recommends the need to have a binding and working framework on mutual legal assistance in addressing cybercrimes in the Community.

Tikk and Kaska[29] stress the significance of cooperation among the States in tackling cybercrimes whose perpetrators are usually located in different countries. The lack of a legal mechanism or political willingness to cooperate equally results in the inability of the Victim State to prosecute the cyber incidents.[30] The authors conclude that the situations where a nation is depending on another sovereign's mercy may, in combination with the persistent trend of politically motivated cyber-attacks, lead to a sense of fearless among patriotic hackers. [31] This article cements the significance of the EAC to forge cooperation which may only be possible through EAC common or shared legal framework as recommended in this study.

Mitchell[32] has it that African governments and corporations are facing the prospect of having to invest hugely in digital security, as cyber-attacks are becoming a much greater threat to the region and its Internet traffic is doubling every 18 months.[33]

By the end of 2020, 495 million people in sub-Saharan Africa subscribed to mobile services – representing 46% of the region's population – an increase of almost 20 million on 2019, according to GSMA, a telecommunications association.[34] By the same time, 303 million people in the region were connected to the mobile internet. Registered mobile money wallets in Africa topped 621 million in 2021 – a 17% increase on 2020.[35] The value of Africa's mobile money transactions jumped by 39% to $701.4bn in 2021.[36] Regardless of enriching this study with how Africa is becoming the go to continent for cyber-attacks, the author does not critically consider the vitality of the mutual legal assistance as a potential tool that may, if effectively crafted and used by the regional communities such as EAC, help to combat all forms of crimes dependent on online environment. The author makes a case for the establishment of a regional monitoring mechanism within the AU framework to improve the regional harmonization of cyber security.

Osula[37] writes on the role of mutual legal assistance and other established mechanisms of international cooperation in the fight against cybercrime. Her analysis is limited to mechanisms facilitating access to

[28]Bailey, E.C, op. cit.
[29] Tikk, E & Kaska K, Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons, available at https://www.ccdcoe.org/uploads/2010/07/Legal_Cooperation_to_Investigate_Cyber_Incidents_Estonian_Case_Study-and_Lessons.pdf, p. 288. Accessed on 10th May 2023.
[30] Tikk, E & Kaska K, Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons, available at https://www.ccdcoe.org/uploads/2010/07/Legal_Cooperation_to_Investigate_Cyber_Incidents_Estonian_Case_Study-and_Lessons.pdf, p. 288. Accessed on 10th May 2023.
[31] Idem.
[32] Jason Mitchell, Africa Faces Huge Cybercrime Threat as the Pace of Digitalisation Increases, the Investment Monitor, 16 June 2022.
[33] Ibid
[34] Ibiden.
[35] Idem
[36] Id.
[37] Osula, A, Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data, *Masaryk University Journal of Law and Technology*, Vol.9, Issue No.1, pp.43-64, p.43.

extraterritorially located data especially during investigation. The author pleads alternative cooperation mechanisms for trans-border data access as a means to ease difficulties in accessing investigative information through the current mutual legal assistance procedures.[38]In contrast, the study covers the State of the legal framework governing the mutual legal assistance under the umbrella of the EAC and whether the established joint or collaboration would work to combat cybercrimes.

Orji[39] discusses international cooperation on cybersecurity within African sub-regional legal instruments and the African Union (AU) Cyber Security Convention.[40] It examines specific directives, model bills, and laws related to cybersecurity within the Economic Community of West African States (ECOWAS), the Common Market for Eastern and Southern Africa (COMESA), and the Southern African Development Community (SADC). The paper highlights the existing challenges in international cooperation and mutual assistance in the AU Cyber Security Convention, and it suggests proposals to strengthen cooperation among African states. The COMESA Model Cybercrime Bill and the SADC Model Law on Computer Crime and Cybercrime provide guidance for developing cybersecurity laws but do not impose international cooperation obligations. Member states using these models must establish separate bilateral arrangements for international cooperation. SADC member states can rely on existing mutual assistance and extradition protocols for cooperation. The author proposes to strengthen international cooperation within the AU include creating additional protocols within the AU Cyber Security Convention to facilitate mutual assistance and international cooperation among member states. He also suggests considering the establishment of a regional Computer Emergency Response Team (CERT) or network security agency to enhance regional cybersecurity efforts. Comprehensively, the author highlights the need for a more comprehensive framework for international cooperation in African cybersecurity. Despite its exhaustive approach, the author has demonstrated quiet comprehensive solutions to the mutual legal assistance in various regional integrations, however the author has not stressed about EAC which this study has covered.

In a snapshot, authors of the reviewed literature discuss the impact brought by the cybercrimes and the need for the States to join hands in ensuring that these crimes are addressed. The general view is that no country is capable of fighting against cybercrimes in its own. Collaboration is, therefore, fundamental in curbing this modern crime. However, there are some limitations noted from each literature which form basis for this study and other future studies. The notable challenge is with respect to the effective coverage of all States forming the EAC.

4. Methodology

This research is a descriptive qualitative study with a comparative approach. The researcher selected this research method as it requires deep analysis of the laws which is related to the topic.

The methodology needed an investigation into the different laws which are related to the topic of the research. With this sort of methodology, the documentary review played a great part in which the researcher examines both published and unpublished materials from textbooks, articles, journals, cases,

[38] Ibiden.

[39] Orji J.U, (2015) Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation? In M. Maybaum, A.-M. Osula, & L. Lindström (Eds.), 7th International Conference on Cyber Conflict: Architectures in Cyberspace. NATO CCD COE Publications at pages 111-112. Available at https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf

[40] Ibid at page 111-114

online sources and websites to obtain relevant and necessary information. Further, as the study relied on the qualitative data,[41] data were analysed qualitatively.[42] In legal context, qualitative research it involved the review of legal texts, laws and other public and scholarly documents related to the study.[43] The study deployed both primary and secondary sources of data through documentary review supplemented by interviews. Documentary review involved the reading of the EAC Treaty, conventional model laws, various principal and subsidiary legislations, case laws developed by the High Courts and relevant Supreme Courts in East Africa with respect to mutual legal assistance and cybercrimes. Other secondary materials such as books, journals, and online content also supported the study.

5. Conceptual Framework on Mutual Legal Assistance

To combat cybercrime, this chapter addresses the conceptual underpinnings of Mutual Legal Assistance (MLA) and other recognized cooperation within the East African community. It briefly describing the legal requirements for a successful war against cybercrime before moving on to an examination of both conventional and alternative collaboration mechanisms for trans-border data access. The paper concentrates on the difficulty in getting data under the present MLA processes, given the realistic estimate that the amount of digital evidence to be obtained extraterritorially would only rise with time. It affirms the necessity for states to take more swift actions to facilitate access to transnational data within East Africa. This chapter puts into context various concepts in as far as the study is concerned. At the outset, some terms expounded in this chapter have retained their natural or dictionary or primary meaning or statutory interpretation whereas other terms have not. All is by design and as per the requirement of the study. On that basis, all terms as defined in this chapter must only be understood in context of the entire study.

a. Computer

A computer is an instrument or a device performing automatically logical operations, depending on the needs of the user at the meantime on what he or she wants to achieve.[44]Despite various useful uses of the computers, some of the users deploy them at the disadvantage of so many innocent users of internet. It is evident that the increasingly use of the computers impacts the nature and level of commission of the cybercrimes. As the technology grows, cybercriminals are also advancing or levelling up the manner of committing their crimes in an online environment.[45]

b. Crime and cybercrime

Crime may be defined as a punishable act. If committed in an online environment, a crime becomes a cybercrime. Cybercrime or computer-oriented crime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime.[46] It is an illegal activity characterized

[41]Qualitative, or non-numerical, legal research involves extracting information from the text of court documents, then interpreting and organizing the text into categories, and using that information to identify patterns. Accessed on https://law.indiana.libguides.com/dissertationguide.
[42] Ibid.
[43] Hoercke, M.V and Ost, F, *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline*? Hart Publishing Ltd, Oxford, 2011, pp.10-11.
[44] Oxford English dictionary (www.oed.).
[45] Ibid.
[46] Hakeem J. Pallangyo, Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services, Tanzania Journal of Engineering and Technology, Vol. 41 (No. 2), June 2022.

by the use of computer as the tool to commit a crime or software to commit digital crime,[47] in other terms cybercrimes may be referred to as the illicit activity carried out through the use of computer as an instrument.[48]A computer crime may also be defined as a crime in which the actors maliciously commit the crime regardless of the respective borders via the use of computer devices.[49] To simply put, to qualify as a cybercrime, the act needs to be committed through or facilitated by a computer or any computer data.[50]The perpetrators of cybercrimes are may not necessarily be located in the area where the crime happens or its effect takes place. Examples of cybercrimes include credit theft, piracy, money laundering and so many acts of the same nature whereas the victim suffer the loss from cyber-criminal activities.[51]

Perpetrators may be sitting in Kenya, but committing crime in Tanzania. The identity of the perpetrators may also be hard to trace both physically or digitally on account of their locality. The cybercrimes may also not materialize the same time as they are committed in the sense that the cybercriminals are able to dictate and define the time, duration, where and to whom should their criminal actions materialize.

On the account of the foregoing, law enforcers who are dealing with cybercrimes are required to possess high level degree of intelligence and enough resources to navigate through this hurdle. On top of the resources and other capabilities in terms of intelligence, detection or prevention of cybercrimes call for a well-established international cooperation.[52]

c. Types of Cybercrimes

Cybercrimes are being categorized into different forms depending on the context each author decide to support. However, for the purpose of this study cybercrimes referred are being categorized depending on the forms provided for under the Budapest Convention.[53] The following offences are categorized as cybercrimes.

i. Illegal Access

This is the intentional access to the whole or any part of a computer system without right.[54] Normally, an act of illegal access is being committed for the purposes of infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.[55]

ii. Illegal Interception

Illegal interception is an act committed intentionally without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.[56]

[47] Ajayi E.F.G Challenges facing the enforcement of cybercrime laws and policy: Journal of internet and information School of law, Kenya University, Nairobi July 25, 2016.
[48] Kirwan D. (2017), An investigation of attitudes and environment factors that make people willing to participate on online crimes, dissertation, master's degree at Dublin institute of technology.
[49] Ashworth A. (1995), Principles of Criminal law Oxford: Clarendon Press, at p.83.
[50] Anthony Reyes, New York city police department's computer crime detective on crime investigation and prosecution of cybercrimes at p. 24.
[51] Ibid.
[52] Ibid at p. 24 of the Anthony Reyes, New York city police department's computer crime Division.
[53] ETS 185 – Cybercrime (Convention), 23.XI.2001 accessed through https://rm.coe.int/1680081561 on 8th September 2023
[54] Article 2 of Council of Europe Convention on Cybercrime
[55] Ibid
[56] Article 3 of Council of Europe Convention on Cybercrime

iii. Data Interference

For the purpose of prosecuting an offender accused of committing a cybercrime of data interference, it is a requirement that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.[57] The offence of data interference may be committed when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right and that the act must have resulted into a serious harm.[58]

iv. System Interference

Most states have implicated the conduct any person in case committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. [59] In most cases, system interference is being invoked for the purpose of accomplishing an evil act such as unlawful money transfers without authorisation of the recognised user.

v. Misuse of Devices

The misuse of a computer device is a cybercrime which entails an act which, when committed intentionally and without right, a the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 of the Budapest Convention through a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established with intent that it be used for the purpose of committing any of the offences,[60] However, to protect intellectual property rights, the application and interpretation of the cybercrime criminalised as misuse of devices, there is provision establishing exception that such prohibition shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession.[61]

vi. Computer-related Forgery

It is globally recognized that when a person intentionally commit and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.[62] Moreso, it is agreeable that for the offence of computer-related forgery to be established, prosecution machinery must prove an intent to defraud, or similar dishonest intent, before criminal liability attaches.[63]

vii. Computer-related Fraud

The cyber-offence of computer fraud occurs when committed intentionally and without right, the causing of a loss of property to another person by any input, alteration, deletion or suppression of computer data, any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.[64]

[57] Article 4 of Council of Europe Convention on Cybercrime
[58] Article 4 of Council of Europe Convention on Cybercrime
[59] Article 5 of Council of Europe Convention on Cybercrime
[60] Article 6 of Council of Europe Convention on Cybercrime
[61] Ibid
[62] Article 7 of Council of Europe Convention on Cybercrime
[63] Ibid
[64] Article 8 of Council of Europe Convention on Cybercrime

viii. Child Pornography

Child pornography is a serious computer crime whereas the acts that are prohibited under this category of cybercrime are producing child pornography for the purpose of its distribution through a computer system, offering or making available child pornography through a computer system, distributing or transmitting child pornography through a computer system, procuring child pornography through a computer system for oneself or for another person, possessing child pornography in a computer system or on a computer-data storage medium. [65] As it is a very serious offence, child pornography includes pornographic material that visually depicts, a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct, realistic images representing a minor engaged in sexually explicit conduct.[66]

ix. Cyberbullying

It is also worth noting the crime of cyberbullying, which is the sending of intimidating or threatening messages, often via social media, and which is pervasive among children and young adult. [67] According to the United Nations Children's Fund (UNICEF): Cyberbullying can take place on social media, messaging platforms, gaming platforms and mobile phones.[68] It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Some of the notable forms of cyberbullying include spread of lies about or posting embarrassing photos of someone on social media; sending hurtful messages or threats via messaging platforms; impersonating someone and sending mean messages to others on their behalf. Face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying leaves a digital footprint a record that can prove useful and provide evidence to help stop the abuse.[69]

d. Mutual Legal Assistance

Mutual legal assistance can simply be defined as a process where states aid one another in gathering evidence and judicial documents in criminal cases.[70] Letters rogatory has been a traditional tool for mutual legal assistance where a state requests another to perform one or more specific action, including collecting evidence and interviewing witnesses on behalf of the requesting state. Having legislation in place makes cooperation easier and so at the convenience of a state there are bilateral, multilateral and regional treaties.[71]As explained, mutual legal assistance in criminal matters entails a process in which State seeks and provides assistance in gathering evidence for use in criminal cases from other States. The mutual legal assistance may be requested for purpose of taking evidence or statements from persons, effecting service of judicial documents, executing searches, seizures and freezing, examining objects and sites, providing information, evidentiary items and expert evaluations, providing originals or certified copies of relevant documents and records including government, bank, financial, corporate or business records, identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes, facilitating the voluntary appearance of persons in the requesting State party and any other type of assistance that is not contrary to the domestic law of the requested State party.[72]

[65] Article 9 of Council of Europe Convention on Cybercrime
[66] Ibid
[67] https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-7-Cybercrimes.pdf.
[68] https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-7-Cybercrimes.pdf.
[69] https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-7-Cybercrimes.pdf.
[70] https://landportal.org/book/narratives/2022/tanzania.
[71] https://fbattorneys.co.tz/cyber-attacks-how-the-tanzanian-laws-protect-us/
[72] United Nations Office on Drugs and Crimes, Manual on Mutual Legal Assistance and Extradition, United Nations Office, Vienna, 2012, p.19 and www.unodc.org.

Cybercrime is rampant in EAC and in which case cooperation among the member states is inevitably due.[73]To prevent more devastating impact of these crimes, there is a need to make comprehensive, and harmonized principles across the region.[74] Through cooperative regional instruments, prosecution machineries across the region will be able to act pursuant to the agreed instruments and hence able to procure the required assistance be it in form of evidence, search, or seizure across their domestic boarders. This will certainly ensure that cybercriminals do not find EAC a safe haven for cybercrimes.[75]

a. **Requesting and Requested Authority**

Requesting authority is the central body entrusted to undertake the process of legal assistance successful from the beginning to the end.[76]In most cases, the requesting authority is the Attorney General. The requesting authority is duty bond to initiate the request and ensure that all mandatory requirements of the law are complied with for that purpose.[77] On part of the requesting State, the request is known as the outgoing request and conversely for the requested State, the request is the incoming request.[78]Upon receiving the requests made, the central authority entrusted with the duty to deal with the request is required to execute the process and ensure that the needs of the requesting states are accommodated on basis of mutual assistance but in a way that does not conflict the applicable domestic rules. The mode of executing the request may be by way of freezing, seizure, confiscation of proceeds of crimes, and detaining a person in transit.[79]

e. East African Community (EAC)

EAC is a regional intergovernmental organization of seven (7) Member States, comprising Burundi, Democratic Republic of Congo, Kenya, Rwanda, South Sudan, Tanzania and Uganda, with the headquarter in Arusha, Tanzania.[80] As stated in chapter one, this study is limited to five (5) East African Community (EAC) Member States including the United Republic of Tanzania, Uganda, Kenya, Rwanda, and Burundi (the selected Member States). Democratic Republic of Congo and South Sudan are out of scope for being largely new to the EAC.

f. Status of Cybercrimes in EAC

On 18 July 2022, Emmanuel Ugirashebuja, the Minister of Justice and Attorney General of the Republic of Rwanda, had it that law enforcement agencies must step up by enhancing measures to detect and prevent the cyber-attacks from the source, where investigation and prosecution can take place.[81] He made this call during the 9th Africa Working Group meeting on Cybercrime for heads of units, in Kigali. The Rwanda Investigation Bureau (RIB) and Interpol were also involved.[82]

According to Ugirashebuja, cybersecurity is an issue of profound importance in today's technology-driven world, a fact of life for all of us, however as the world continues to recover from the disruptions caused by the Covid-19 pandemic, practices including the increased use of virtual workspaces, online

[73] East Africa Community Draft on Mutual Legal assistance on cyber laws of 2008.
[74] African Union Commission.
[75]Asherry Magalla, Manual on Tanzania laws on Mutual Legal Assistance on criminal Matters at p. 15.
[76] Asherry Brian Magalla, a Manual on Mutual Legal assistance on criminal matters, at p.14 of the book which detailed clearly the way process should be undertaken by the requesting state party so as to make the move successes in a satisfactorily.
[77] Ibid.
[78] Ibid Op. Cit at p. 15.
[79] See Part I, II and IV of the United Nations, Model Laws on criminal crime of 2007, Office of Drugs and Crime.
[80]https://www.eac.int.
[81]https://www.minijust.gov.rw/news-detail/law-enforcement-agencies-must-step-up-by-enhancing-measures-to-detect-and-prevent-the-cyber-attacks-from-the-source.
[82]Ibid

marketplaces and e-Governance have become the norm. While this presents opportunities to revamp economies and streamline public service delivery in general and justice in particular, it unfortunately and simultaneously increases exposure to cybercrime.[83]

According to the 2021 Interpol cyber threats assessment report, the highest-reported and most pressing cyber threats across the region was identified as online scamming. This targets and takes advantage of victims' fears, insecurities, and vulnerabilities through phishing, mass mailing and social engineering. There is also a sharp increase in the number of online banking scams, including instances of banking and credit card fraud.[84]

The speed of technological advancement, increasing globalisation, and exponential growth of global markets have created opportunities for criminal activities using new forms of anonymity often with low-risk detection. As technology continues to evolve, so do the opportunities and challenges it provides.

The report also indicates that digital extortion is also rampant in Africa and it targets individuals with either allegation of sexually compromising images or through direct blackmail campaigns. The move towards a digital society - particularly within Africa has created new attack vectors for criminals to both cloud their identity and target new victims. Alongside online scams, Business Email Compromise (BEC) was also identified as a significant concern and threat to Africa as indicated in the Interpol report. Businesses and organizations that rely heavily on wire transfer transactions are vulnerable to this threat in Africa. Interpol claims also that the COVID-19 pandemic has contributed to the increase in this type of cybercrime.

Statistics show that 90% of African businesses in Africa are operating without the necessary cybersecurity protocols in place but this has not stopped attacks from happening. A research study from Deloitte estimates that the financial loss for financial institutions in Kenya, Rwanda, Uganda, Tanzania, and Zambia since 2011 to be more than US$ 245 million.

Since 2018, RIB has handled 256 cases of cybercrimes that involved a total of Rwf 1,647,963,709 and US$ 659,280. The highest number of cases were recorded in the year 2020-2021 and they totaled to 254 cases. However, the year 2019-2020 had cases with the biggest amount stand at Rwf 1,027,567,721 and US$ 417,586. Based on the foregoing, it is evident that cybercrime attacks are rampant across EAC. In June, an entire DDoS campaign was discovered targeting financial and government institutions in Uganda. Among the victims were the Bank of Uganda, the stock exchange, the parliament, as well as many ministries.[85] Earlier in 2023, cyberattacks increased by 76% across Kenya in particular, with exploits emerging as the most dominant form of attack in the nation.

More particularly, sometimes in mid-July, Kenya endured a huge cyber-attack that affected services on a key government online platform. BBC reported a cyber-attack against the region's eCitizen portal used by the public to access over 5,000 government services. Impacted were passport applications and renewal, e-visas for non-citizens visiting Kenya, as well as driving licences, ID cards and health records from being issued.[86]According to the government there have been galloping rise in cybercrimes in Burundi, statistics indicates at least 1373 complaints were made in 2018 and rose to 6123 in 2019, 6894

[83]https://www.minijust.gov.rw/news-detail/law-enforcement-agencies-must-step-up-by-enhancing-measures-to-detect-and-prevent-the-cyber-attacks-from-the-source.
[84] https://allafrica.com/stories/202207190053.html.
[85] https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/
[86] Kenya cyber-attack: Why is eCitizen down? - BBC News.

in 2020 and 7532 in 2021. In 2018 at least 462 people were arrested while 126 people were sentenced for cybercrime related charges.[87]

3.1 Legal Framework on Mutual Legal Assistance in Combating Cybercrimes in the EAC

The increasing desire to communicate in a paperless mode for the people working in numerous fields is an aftermath of technological development. As the technology shoots, so does the number of cybercrimes. The manner in which the criminal justice delivery system was set to function must also change in order to accommodate or embrace the technological advancement. The changes in criminal justice delivery system are necessary to enhance justice in the digital era. International and regional communities have been pioneering the move by coming up with models and guidelines aiming at addressing challenges posed by digital era in relation to collaboration in combating cybercrimes within the EAC. In this chapter, the laws governing mutual legal assistance in combating cybercrimes at international, regional and domestic level are discussed and analysed as below.

Legal Framework on Mutual Legal Assistance in Cybercrimes

a. International Instruments

At the United Nations level, there is no single legal instrument that addresses matters of cybercrimes. However, Since May 2021, UN member states have been negotiating an international treaty on countering cybercrime. If adopted by the UN General Assembly, it would be the first binding UN instrument on a cyber-issue.[88] The treaty could become an important global legal framework for international cooperation on preventing and investigating cybercrime, and prosecuting cybercriminals.[89] But without a clearly defined scope and sufficient safeguards, the treaty could endanger human rights – both online and offline – and repressive governments could abuse its provisions to criminalize online free speech.[90] It could also threaten digital rights by legitimizing intrusive investigations and unhindered law enforcement access to personal information.[91] However, the United Nations Office of Drugs and Crimes (UNDO) provided for a model law of the fight against cybercrimes. The Model Law is not binding in nature, however, provides for the guidance on how state parties may invoke relevant efforts to combat cybercrimes. On the other hand, effective guidelines from well developed countries are being referred as they offer best practice in the war and combating of cybercrimes.

i. Council of Europe Cybercrime Convention, (Budapest convention) of 2001

Despite absence of the clear legal instrument under the realm of United Nations focusing on providing proper mechanism in combating cybercrime globally, the Budapest Convention set playground for the world to combat and fight cybercrimes. The Convention provides for significant aspects of cybercrimes whereas under Chapter I provides for various definition connected to cybercrimes.[92]

[87] https://www.burunditimes.com/burundi-passes-tough-law-on-cybercrime.
[88] https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter accesses on 9 October 2023
[89] Ibid
[90] Ibid
[91] https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter accesses on 9 October 2023

[92] Article 1 of The Budapest Convention on Cybercrimes provides for definition of key terms such as "computer system" to mean any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data,' "computer data" to mean any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function, "traffic data" to mean any computer data relating to a communication by means of a computer system, generated by a computer

According to article 25,[93] The member states to the Convention commits themselves to offer cooperation at a widest extent for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.[94] Further, member states are compelled and mandated to adopt such legislative and other measures as may be necessary to carry out the obligations in respect of mutual legal assistance.[95] Moreover, the Convention provides for the urgent situation that, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e- mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. To operationalise the requested party, the latter is put under obligation to accept and respond to the request by any such expedited means of communication.[96] To appreciate the principle of sovereignty, mutual assistance a conditional precedent was set that subjest to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. To effectuate the MLA procedure and its effectiveness, the Convention creates mandatory duty to the member states to respond to the request of another member state. Under the Convention, the requested party is not into exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11[97] solely on the ground that the request concerns an offence which it considers a fiscal offence.

Model Law on Mutual Assistance in Criminal Matters[98]

The MLMACM was introduced to enhance cooperation in the fight against cybercrimes.[99] The MLMACM defines criminal matter to include any investigation, prosecution or judicial proceeding relating to: (a) any criminal offence; or (b) the determination of whether property is proceeds or instrumentalities of crime or terrorist property; (c) a possible confiscation order, whether or not based on an underlying criminal conviction; or (d) the freezing or seizure of proceeds or instrumentalities of crime or terrorist property, (e) an investigation carried out by an administrative investigative body with a view to referral for prosecution under the criminal law. The object of the MLMAC is to facilitate the widest range of assistance to be given and received by the requesting state in investigations, prosecution and judicial proceedings in relation to criminal matters, including with respect to the freezing, seizing and confiscation of proceeds and instrumentalities of crime and terrorist property across countries.Other forms of providing assistance including controlled delivery, joint investigations, and the use of other special investigative techniques and the transfer of criminal proceedings are also permitted. Despite being illustrative in terms of directing how mutual assistance in criminal matters can be undertaken, this

system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

[93] The Budapest Convention, 2001

[94] Article 25(1) of The Council of Europe Convention on Cyber.

[95] Article 25(2) of The Counsel of Europe

[96] Article 25(3) of The Budapest Convention

[97] The Budapest Convention, 2001

[98] The model law was established by the United Nations Office on Drugs and Crimes which is an office responsible for combating and fighting of transnational crimes.

[99] Elaborated in the Vienna based United Nations Office on Drugs and Crime, Division for Treaty Affairs, Treaty and Legal Affairs Branch (UNODC/DTA/TLAB) in accordance with General Assembly resolution 53/112 of 9 December 1998.

model law is not binding to the EAC Member States as so far there is nothing in the model law which is reflected in any of the EAC instruments.

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002[100]

The 200 Guidelines introduced a fundamental paradigm shift in the way IT security was previously addressed, in order to take into account, the emergence of the open Internet and the generalisation of interconnectivity. The underlying reasons for the 2002 Guidelines include but not limited to the fact that: (a) the data and information stored on and transmitted over information systems and networks are subject to threats from various means of unauthorised access, use, misappropriation, alteration, malicious code transmissions, denial of service or destruction and require appropriate safeguards; and (b) a common interest in promoting the security of information systems and networks by means of a culture of security that fosters international co-ordination and co-operation to meet the challenges posed by the potential harm from security failures to national economies, international trade and participation in social, cultural and political life.[101]

The guidelines are non-binding Guidelines and, unlike conventions, governments are not legally bound by these Guidelines.[102] The nine principles set out in the Guidelines reflect the agreed position of OECD countries and have the support of the international business community and consumer protection organisations. Member governments are also committed to implementing the Guidelines.[103] The key aim of the 2002 Security Guidelines is to provide governments, business and individual users with guidance for protecting the security of information systems and networks in a climate of increasing potential threat to these systems, and to provide a common international approach to creating a worldwide "culture of security". [104]

The 2002 Guidelines created a framework for security to remain effective in an open, dynamic and unpredictable technical environment where participants reduce risk before accepting it, instead of avoiding risk by limiting interconnectivity. The 2002 guidelines were introduced to make an appeal to the member states to develop security system and privacy for their information systems in countering cybercrimes commission which seemed increasing.[105]

Irrespective of the fact that the 2002 guidelines reiterate the significance of cooperation among the states in fighting against cybercrimes, this has not been implemented in East Africa.

[100] These guidelines have been provided for by the United States Department of Justice as a mechanism to respond to the cybersecurity threats. The 2002 Security Guidelines were adopted by the OECD Council on 25 July 2002 and are currently in effect. The OECD Press Release of 7 August 2002 launches the Security Guidelines Awareness Campaign.

[101] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002, p.13 and 14.

[102] https://www.oecd.org/digital/ieconomy/2494779.pdf accessed on 14th October 2023

[103] https://www.oecd.org/digital/ieconomy/2494779.pdf accessed on 14th October 2023

[104] Ibid

[105] OECD (2012-11-16), "The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy", OECD Digital Economy Papers, No. 209, OECD Publishing, Paris.

a. Regional level

i. African Union Convention on Cyber Security and Personal Data Protection[106]

Malabo Convention covers more than electronic transactions and personal data protection but as well it addressed adequately, in wide, the need for cybersecurity and mutual legal assistance between and within member states. This gives this Convention a unique and innovative character among cybersecurity-related regulations and policies. It is, however, also the reason for some of the challenges regarding its ratification.

This Convention has been motivated by the tremendous growth of the internet use in Africa, the Convention imposes obligations on Member States to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime.[107] This treaty is referred to as the African Union (AU) Convention on Cyber Security and Personal Data Protection.

Article 28 of the Convention addresses the issue of cybercrimes and the need for mutual legal assistance as the mechanism to combat cybercrimes. Article 28(2) provides for International Cooperation on issues of cybercrimes, that is member states shall enter into agreements to create a favourable environment for mutual legal assistance in cybercrimes.

The provision of the Convention gives member states the obligation to cooperate and unite in combating cybercrimes, it encourages mutual legal assistance between member states. It is worth to note that, as of 19th September 2023, out of 55 African Union members, 19 have signed the convention, and 15 ratified it and deposited instruments of ratification with the AU.[108] Countries that have ratified the convention: Angola, Cabo Verde, Republic of the Congo, Djibout, Mauritania, Ghana, Guinea, Mozambique, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo, Zambia.[109] The only East African country that have ratified it is Rwanda leaving Burundi, Uganda, Kenya and Tanzania out of scope.[110]

ii. Common Markets for Eastern and Southern Africa (COMESA)

Preferential Trade Area for Eastern and Southern Africa was transformed into Common Markets for Eastern and Southern Africa in 1994.[111] COMESA has impliedly addressed the issue of cybercrime via Article 3(d) of the Treaty establishing the Common Markets for Eastern and Southern Africa as one of its objectives, where it states that state parties must should co-operate in the promotion of peace, security and stability among the Member States in order to enhance economic development in the region. To accomplish this, COMESA through its official gazette dated 15th October 2011 has made a policy on cyber security which in turn enables mutual legal assistance on cybercrimes the decision of the council. These include to come up with the Model Cyber Security Policy, Model Bill, Cyber Security Implementation Roadmap respectively be adopted; and The COMESA Secretariat as the Chairperson of the Tripartite Task Force to undertake the harmonization of the cyber security policies within the tripartite framework. This was an initiative aiming to guide member state to creating their own laws to govern cybercrime, however, the Bill does not establish any binding obligations on Member States to

[106] This Convention is commonly referred to as The Malabo Convention which was adopted by the twenty-third ordinary session of the AU Assembly held in Malabo, Equatorial Guinea, 27th June 2014.
[107] Ibid.
[108] https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection accessed 14th October 2023
[109] Ibid
[110] https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection accessed 14th October 2023
[111] https://au.int/en/recs/comesa#:~:text=The%20PTA%20Treaty%20envisaged%20its,Malawi%20on%208th%20December%201994. Accessed on 15th October 2023

criminalize cybercrimes and the same is still a challenge as not all member states have adopted laws governing cybercrime nor mutual legal assistance.[112]

b. Southern Africa Development Community (SADC)

SADC is a Regional Economic Community comprising 16 Member States, Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic Tanzania, Zambia and Zimbabwe.[113] The mission of SADC is to promote sustainable and equitable economic growth and socio-economic development through efficient, productive systems, deeper cooperation and integration, good governance and durable peace and security; so that the region emerges as a competitive and effective player in international relations and the world economy.[114] The main objectives of Southern African Development Community (SADC) are to achieve economic development, peace and security, and growth, alleviate poverty, enhance the standard and quality of life of the peoples of Southern Africa, and support the socially disadvantaged through Regional Integration. These objectives are to be achieved through increased Regional Integration, built on democratic principles, and equitable and sustainable development. The objectives of SADC, as stated in Article 5 of the SADC Treaty (1992) are to: Achieve development and economic growth, alleviate poverty, enhance the standard and quality of life of the people of Southern Africa and support the socially disadvantaged through Regional Integration, evolve common political values, systems and institutions, promote and defend peace and security, promote self-sustaining development on the basis of collective self-reliance, and the inter-dependence of Member States, achieve complementarity between national and regional strategies, promote and maximize productive employment and utilization of resources of the region, achieve sustainable utilization of natural resources and effective protection of the environment, strengthen and consolidate the long-standing historical, social and cultural affinities and links among the people of the Region.To fulfil its mission in relation to collaboration in the areas of science and technology and politics, diplomacy, international relations, peace and security, SADC has developed various model laws.[115]

These model laws are intended to strengthen the aimed of the Member States to come together in dealing with matters of science and technology including the matters of cyber space. These model laws include the SADC.

c. Economic Community of West African States (ECOWAS)

In 2021, the Economic Community of West African States (ECOWAS) adopted its Regional Cybersecurity and Cybercrime Strategy, outlining actions to be taken in particular at national level to strengthen cybersecurity and fight cybercrime such as adoption of national cybersecurity strategies, establishing dedicated authorities, prioritizing cybersecurity efforts in the area of critical infrastructures and essential services, enhancing cybersecurity skills development, and building capacity against cybercrime).[116]

[112] https://www.comesa.int/wp-content/uploads/2020/05/2011Gazette-Vol.-16.pdf accessed on 15th October 2023
[113] https://www.sadc.int/member-states accessed on 15th October 2023
[114] Ibid
[115] https://www.sadc.int/.
[116] Orji J.U, (2015) Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation? In M. Maybaum, A.-M. Osula, & L. Lindström (Eds.), 7th International Conference on Cyber Conflict: Architectures in Cyberspace. NATO CCD COE Publications at pages 112-113 Available at https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf

When it comes to foreign policy issues, member states and the ECOWAS Commission are invited to promote and develop regional and international cooperation through actions such as sharing alerts and cybersecurity information (in particular between CERTs and similar institutions and ensuring international judicial cooperation on cybercrime and transnational access to digital evidence.[117]

ECOWAS's Regional Critical Infrastructure Protection Policy proposes preventive, reactive, and proactive measures that countries could take to ensure the protection of their critical infrastructures and essential services.[118] Noting that there are 'interdependencies between countries' in relation to telecommunication networks, internet connectivity, and other infrastructure and services, the policy calls on countries to cooperate in identifying transitional critical infrastructures and essential services, exchange information on threats and risks, and harmonize protection measures. Moreover, ECOWAS also has a Cybercrime Directive (adopted in 2011); its objective is to ensure that the criminal law and criminal procedures of ECOWAS member states are adequately equipped to address cybercrime.[119]

8. **EAC Legal Framework for Cybercrime Laws**

a. East Africa Community Treaty of 1999

The EAC Treaty was signed in Arusha by the three founding member states that are Tanzania, Kenya and Uganda on the 30 November 1999.[120] The Treaty entered into force on 7 July 2000. In the context of mutual legal assistance, Article 124(5) of the Treaty creates specific provisions on that regard.

In the context and dictates of article 124(1) of The Treaty, member states undertook to cooperate in reviewing the region's security particularly on the threat of terrorism and formulate security measures to combat terrorism. Through the above provisions, the EAC Treaty contains the provisions which recognise the necessity of mutual assistance in preventing, eliminating and prosecuting cybercrimes in the EAC.

The vision of regional integration in East Africa is to create wealth, raise the living standards of all people of East Africa and enhance international competitiveness of the region. The key to achieving this vision is increased production, trade and investments in the region with Information and Communication Technologies (ICT) playing a leading role. The information and knowledge-exchange driven third millennium requires reliable ICT services as a key national and regional resource. Furthermore, the EAC Treaty emphasises cooperation to achieve coordinated, harmonized, and complementary infrastructural development.[121]

The Framework for Cyber laws ("Framework") was prepared by the East African Community EAC Task Force on Cyber laws, comprising representatives from the Partner States and the EAC Secretariat, with the support of UNCTAD. The Framework contains a series of recommendations made to the governments of the partner states about reforming national laws to facilitate electronic commerce; to facilitate the use of data security mechanisms; to deter conduct designed to undermine the confidentiality, integrity and availability of information and communication technologies; to protect consumers in an online environment, and to protect individual privacy. The recommendations are

[117] Ibid
[118] Ibid
[119] https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/cybersecurity-cybercrime-africa-continentalregionalpolicies/#:~:text=Out%20of%2055%20AU%20members,(as%20of%20March%202022).&text=Countries%20that%20have%20ratified%20the,%2C%20Senegal%2C%20Togo%2C%20Zambia.
[120] https://www.eac.int/eac-history accessed on 15 October 2023
[121] Draft Eac Legal Framework For Cyberlaws, 2008, P.3.

designed to harmonise the law reform process between the EAC Partner States, as well as reflecting international best practice.

Despite the foregoing, the EAC Treaty by itself is not comprehensive to fully guide the Member States in rendering cooperation among themselves in fighting against cybercrimes. Consequently, the request for mutual assistance takes so long to yield the intended objectives and becomes more ineffective considering the fragile nature of cybercrimes and nature of electronic evidence.

d. Domestic Legislations in EAC

Each member of the EAC has and maintain separate mutual assistance in criminal matters. In Tanzania, the mutual assistance in criminal matters is governed by the Mutual Assistance in Criminal Matters Act (the **MACMA**).[122]The MACMA provides for mutual assistance in criminal matters between Tanzania and foreign countries; to facilitate the provision and obtaining by Tanzania of such assistance and to provide for related matters. According to section 4 of the MACMA, the mutual assistance in criminal matters include: (a) the obtaining of evidence, documents or other articles; (b) the provision of documents and other records; (c) the location and identification of witnesses or suspects; (d) the execution of requests for search and seizure; (e) the making of arrangements for persons to give evidence or assist in investigations; (f) the forfeiture or confiscation of property in respect of offences; (g) the recovery of pecuniary penalties in respect of offences; (h) the restraining order of dealings in property, or the freezing of assets, that may be forfeited or confiscated, or that may be needed to satisfy pecuniary penalties imposed, in respect of offences; (i) preserving and obtaining all forms of computer and telecommunication data; (j) interception of postal items; (k) interception of communications data; (l) covert electronic surveillance; (m)facilitating the taking of evidence by video conference; (n) carrying out undercover operations and controlled delivery; (o) the location of property that may be forfeited, or that may be needed to satisfy pecuniary penalties imposed, in respect of offences; and (p) the service of documents. Kenya is a signatory to several Bilateral and Multilateral Mutual legal assistance (MLA) treaties and agreements that provide for international cooperation in criminal matters. Kenya can provide mutual legal assistance based on the principles of reciprocity and mutual cooperation. Kenya is a member of the Commonwealth, Harare Scheme and London Scheme relating to Mutual legal assistance in criminal Matters within the Commonwealth. The domestic law for mutual legal assistance is the Mutual Legal Assistance Act, Act No. 36 of 2011 of the Laws of Kenya. Kenya can provide MLA to any country or territory in the world whether or not there is such an agreement. Kenya would, however, expect reciprocity from countries to which we give assistance. Where an agreement imposes specific conditions or procedures, Kenya expects these to be adhered to.[123] Uganda is a common law country with very limited legislation on extradition and MLA. Extraditions are managed under the Extradition Act, which a very old law of 1964. Unlike states like Tanzania that have legislation on MLA, Uganda still relies on the Common wealth scheme on MLA. The recent wave of international crime, particularly terrorism has necessitated the need to urgently develop the much-needed legislation both at national and regional level. In Uganda, this wave of crime has necessitated the creation of The International Crimes Division handles crime which falls under the following categories: (i) Terrorism (ii) Human trafficking (iii) War Crimes (iv) Other crimes (like Genocide, crimes against humanity not applied in the on-going

[122] [Cap 254 R.E 2022].

[123] Requests For Mutual legal assistance In Criminal Matters -Guidance For Authorities Outside Of Kenya-2018 accessed through https://statelaw.go.ke/wp-content/uploads/2020/11/MLA-GUIDELINES-IN-CRIMINAL-MATTERS-FOR-AUTHORITIES-OUTSIDE-OF-KENYA.pdf on 29 September 2023

cases and investigation).[124] Uganda is a member state to the Common Wealth Mutual Legal Assistance Scheme.[125]

In Rwanda, the mutual assistance in criminal matters is governed by Government Mutual Legal Assistance in Criminal Matters.[126]The law applies to the request for legal assistance in criminal matters to or from a foreign State in regards to various areas of cooperation.

As outlined above, every state maintains its own mutual assistance in criminal matters and does not specifically deal with cybercrimes.

a. **Analysis**

This part of the paper presents research findings extracted insofar as the study was concerned. The study aimed at examining the status of legislation with regards to mutual assistance in combating cybercrimes; the status of cooperation in investigating, prosecuting, and punishing cybercriminals; and the need for comprehensive, Harmonized, and practical framework on mutual assistance in relation to cybercrimes. The foregone parts, the context of the study has been placed. The data for the study was collected through documentary review and in-depth interviews with the respondents.

i. Status of Legislation on Mutual Legal Assistance in Criminal Matters

In traversing to the objective of examining the status of legislation with regards to mutual assistance in combating cybercrimes, the researcher reviewed various writing and the laws. Apart from reviewing the laws, the responses from two respondents from the national prosecution agencies of Tanzania and Kenya were also obtained. From the documentary review it is evident that each member of the EAC has and maintain separate mutual assistance in criminal matters. In Tanzania, the mutual assistance in criminal matters is governed by the MACMA.[127]

The MACMA provides for mutual assistance in criminal matters between Tanzania and foreign countries; to facilitate the provision and obtaining by Tanzania of such assistance and to provide for related matters. In Tanzania, the mutual assistance in criminal matters include, among other things: (a) the obtaining of evidence, documents or other articles; (b) the provision of documents and other records; (c) the location and identification of witnesses or suspects; (d) the execution of requests for search and seizure; and I the making of arrangements for persons to give evidence or assist in investigations. Rwanda and Uganda also maintain their own separate procedures for implementing mutual assistance in criminal matters that may not necessarily be specific to the cybercrimes. This is an inherent challenge in the mutual assistance framework in EAC.

Kenya is a signatory to several Bilateral and Multilateral Mutual legal assistance (MLA) treaties and agreements that provide for international cooperation in criminal matters. Kenya can provide mutual legal assistance based on the principles of reciprocity and mutual cooperation. Kenya is a member of

[124] Strengthening Judicial Cooperation in the Great Lakes Region: National Frameworks in Light of ICGLR Protocol. 'Uganda's Procedure on Extradition and Mutual Legal Assistance' 19th -20 April, 2016, Nairobi Kenya accessed through https://ungreatlakes.unmissions.org/sites/default/files/uganda.pdf on 29 September 2023.

[125] Commonwealth countries cooperates on mutual legal assistance without the necessity of a treaty. or bilateral agreement between the countries. The Commonwealth is comprised of 54 Member States including: Antigua & Barbuda, Australia, Bahamas, Bangladesh, Barbados, Belize, Botswana, Brunei Darussalam, Cameroon, Canada, Cyprus, Dominica, Fiji, Gambia, Ghana, Grenada, Guyana, India, Jamaica, Kenya, Kiribati, Lesotho, Malawi, Malaysia, Maledives, Malta, Mauritius, Mozambique, Namibia, Nauru, New Zealand, Nigeria, Pakistan, Papua New Guinea, Saint Lucia, St. Christopher & Nevis, St. Vincent & the Grenadines, Samoa, Seychelles, Sierra Leone, Singapore, Solomon Islands, South Africa, Sri Lanka, Swaziland, Tanzania, Tonga, Trinidad & Tobago, Tuvalu, Uganda, United Kingdom, Vanuatu, Zambia and Zimbabwe. https://www.unodc.org/pdf/lap_mlaeg_report_final.pdf accesses on 15 October 2023.

[126] No. 005/2021 of 05/02/2021.

[127] [Cap 254 R.E 2022].

the Commonwealth, Harare Scheme and London Scheme relating to Mutual legal assistance in criminal Matters within the Commonwealth. The domestic law for mutual legal assistance is the Mutual Legal Assistance Act, Act No. 36 of 2011 of the Laws of Kenya. Kenya can provide MLA to any country or territory in the world whether or not there is such an agreement. Kenya would, however, expect reciprocity from countries to which we give assistance. Where an agreement imposes specific conditions or procedures, Kenya expects these to be adhered to.[128]

However, both countries have the specific laws on regulating cybercrimes. In 2015, Rwanda came up with a national cyber security policy that established a National Computer Security and Response Centre. The centre detects, prevents and responds to cyber security threats. And in 2016, the Regulatory Board of Rwanda Utilities rolled out network security regulations to protect the privacy of subscribers. They also empower the government to regulate and monitor internet operators and service providers.[129] Cybercrimes, in Tanzania, are punishable under the Cybercrimes Act (CA) passed in 2015.[130]

The CA makes provisions for criminalizing offences related to computer systems and information communication technologies; to provide for investigation, collection, and use of electronic evidence and for matters related therewith. Some of the acts criminalized include publication of false information, pornographic, and lavish pornographic. However, the CA does not cement on the mutual assistance in the event the commission of the cybercrime in Tanzania is facilitated or undertaken from outside the country despite the fact that the CA has an extraterritorial reach.

The respondents involved were also of the view that the as It stands, each member of the EAC embraces its own legislative framework which is not healthy in mutual legal assistance especially in relation to cybercrimes. Appealing to its nature, the prevention of cybercrimes in EAC calls for the dedicated framework from the local and regional level addressing the manner in which mutual assistance can be implemented, the respondents urged. Overreliance to the traditional approach to the mutual assistance in relation to cybercrimes bear no meaningful results.[131]It has been further contended that as a result of an inconsistent approach to mutual assistance, it becomes problematic for the cybercrimes to be effectively and timely prosecuted.

ii. Status of Cooperation

In relation to the objective of probing the status of cooperation in relation to the fight against cybercrimes among the member states of the EAC, the researcher reviewed various writings and also obtained responses from three respondents from the respective national prosecution offices of Rwanda and Burundi. The guiding question on status of cooperation was do EAC Member States collaborate to investigate, prosecute and punish cybercriminals. Patrick Mwaita and Maureen Awor[132] have documented that Burundi admits that, no country in the world can effectively fight against cybercrime individually. The nature of the phenomenon and especially the highly technical realization suggests that

[128] Requests For Mutual legal assistance In Criminal Matters -Guidance For Authorities Outside Of Kenya-2018 accessed through https://statelaw.go.ke/wp-content/uploads/2020/11/MLA-GUIDELINES-IN-CRIMINAL-MATTERS-FOR-AUTHORITIES-OUTSIDE-OF-KENYA.pdf on 29 September 2023

[129]Mercy Muendo, **what's been done to fight cybercrime in East Africa,** December 2, 2019 4.11pm SAST, accessed through What's been done to fight cybercrime in East Africa (theconversation.com) on 30 September 2023.

[130]Act No.14 of 2015.

[131] Zoom/telephonic interview with (names withheld), public prosecutors held on 23 September 2023 from10:00:00-10:30:00hrs.

[132] Workshop Report on Effectives Cybercrime Legislation in Eastern Africa, Dar es Salaam, Tanzania, 22-24 August 2013, Patrick Mwaita and Maureen Owor (ACCP) Accessed through 16802f2349 (Coe.Int) on 29 September 2023.

all states of the world have to work together to deal with the challenge. The problem of cybercrime is that it is an almost imperceptible offense. The location of the cyber offender is unknown and impractical.[133] The respondents who were asked to comment on the status of cooperation among the EAC member states when it comes to cybercrimes responded to the effect that, due to the scattered or uncoordinated regulations on mutual assistance, the status of cooperation is arguably not satisfactory. The legal regime does not bind the member states to expedite the process and in most cases, it depends on the will of the requested authority and the nature of the relationship between the requesting and the requested authorities.[134] This is the reason why cybercrimes keep flourishing across the region instead of slowing down. Given the legislation status as highlighted above and the responses that the speed or pace at which the requests for the mutual assistance are currently actioned upon depends on the will of the requested authority and the discretion of the member states, it can be said that the level of cooperation is truly not satisfactory.

iii. Needs for a Framework

On the objective to examine the needs for a comprehensive, harmonized, and practical framework on mutual assistance in relation to cybercrimes, the study sought responses from the officers from the cybercrimes departments from Tanzania and Uganda. The guiding question was whether there a need for a comprehensive, harmonized and practical framework on mutual assistance in relation to cybercrimes in the EAC. The researcher also obtained other responses from the documentary reviews.

De Busser[135] opines that the traditional mechanism of mutual legal assistance is losing ground quickly because of its slow and cumbersome way of working. With surveys showing that it takes authorities an average of ten months to react to a request for mutual legal assistance in some cases, no reaction is received at all by the individual requesting authority, as well as the European Union institutions, have sought faster alternatives. Ten months is slow in any criminal investigation even in a domestic setting, but it is unworkably slow when the evidence is in digital rather than in physical or intangible form.[136]

According to the author, the rapid increase of digital evidence for all types of criminal offences – not just computer-related offences – emphasizes the slowness and general inadequacy of the traditional cooperation system. Digital evidence introduces not only a volatile type of information that can be highly relevant to criminal investigations, but also presents a world of territorially organized national criminal laws with the inherently exterritorial world of digital data.[137]

Also, the member states undertake to co-operate in reviewing the region's security particularly on the threat of terrorism and formulate security measures to combat terrorism. Through the above provisions, the EAC Treaty contains the provisions which recognise the necessity of mutual assistance in preventing, eliminating and prosecuting cybercrimes in the EAC.

All respondents who were interviewed in relation to this objective had a view that the current statistics of cybercrimes in EAC calls for the urgent cooperation among the member states in terms of coming up with a dedicated legislation addressing how the mutual assistance in cybercrimes can be jointly achieved in East Africa. The respondents appreciate the significance of the cooperation among the member states

[133] Workshop Report on Effectives Cybercrime Legislation in Eastern Africa, Dar es Salaam, Tanzania, 22-24 August 2013, Patrick Mwaita and Maureen Owor (ACCP) Accessed through 16802f2349 (Coe.Int) on 29 September 2023.
[134] Zoom/telephonic interview with (names withheld), public prosecutors held on 25 September 2023 from10:00:00-10:30:00hrs.
[135] De Busser, E.D, The Digital Unfitness of Mutual Legal Assistance, *Security and Human Rights*, 2017, Vol.28, pp.161-179.
[136] Ibiden
[137]Idem.

pursuant to the definitive legal framework which takes into consideration the context of East African States and its level of development which makes these states more vulnerable to the cyber-attacks.[138]

b. Status of Legislation in Cybercrimes in East African Community

i. Tanzania

The laws applicable for cybercrimes in Tanzania are: Cybercrime Act 2015 is the primary source of substantive law provisions and covers offenses such as illegal access, interception, data interference, and data espionage, among others. The Electronic and Postal Communications Act, 2010 addresses issues such as cybersecurity, interception, encryption, and data retention related to electronic communications. It prohibits several conducts, such as the transmission of obscene content, hate speech, unauthorized access or use of computer systems, and making or sharing false information, to protect consumers.[139]Additionally, the Electronic Transactions Act recognizes and provides for the requirements of digital signature and e-money, which are essential for workers who do not need to be physically present in discharging their duties.[140] The Tanzania Penal Code also provides provisions on intention, motive, theft, impersonation, and false assumption of authority, among others, to protect against cybercrime.

Tanzania gazetted its Cybercrime Act in May 2015. On close reading, it is clear that the legislation borrows from the SADC Model Law. From the above laws, there are no provisions which elaborate, provide or refer to mutual legal assistance process and how cybercrimes may be dealt with in a global level. The above laws only specify protection against and penalizing offences of cybercrimes on a national level.

i. Kenya

The status of cybercrimes legislation in Kenya is somehow exhaustive compared to other EAC member states. On that note, the following are the laws applicable to cybercrime in Kenya: Computer Misuse and Cybercrimes Act, No. 5 of 2018 Laws of Kenya – this is the principal legislation on cybercrimes in Kenya that provides for all offenses relating to computer systems such as unauthorized access or interference, cyber espionage, cyber harassment, cybersquatting, phishing and cyber terrorism; contains provisions to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; and facilitate international co-operation in dealing with computer and cybercrime matters. The other legislation is Kenya Information and Communications Act, No. 2 of 1998 Laws of Kenya (the "KICA") - was amended in 2019 to provide for the regulation of electronic transactions and cyber-security by requiring the Communications Authority of Kenya ("CA") to develop a framework for facilitating the investigation and prosecution of cybercrime offenses and promote and facilitate the efficient management of critical internet resources.[141] Also, Data Protection Act, No. 24 of 2019 laws of Kenya - imposes obligations on data controllers and data processors to provide security measures and mechanisms to ensure the protection of personal data against unlawful destruction, loss, alteration, and transfer.[142] Lastly, Guidelines on Cybersecurity for Payment Service Providers, July 2019 - require Payment Service Providers **(PSPs)** to submit their Cybersecurity Policies to the Central Bank of Kenya and report any cybersecurity incidents that could impact their ability to

[138] Zoom/telephonic interview with (names withheld), public prosecutors held on 25 September 2023 from10:00:00-10:30:00hrs.
[139] https://landportal.org/book/narratives/2022/tanzania
[140] https://fbattorneys.co.tz/cyber-attacks-how-the-tanzanian-laws-protect-us/
[141] https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/kenya.
[142] Ibid.

provide services. PSPs must also provide quarterly reports to the CBK on the occurrence and handling of cybersecurity incidents.[143]

ii. Uganda

The laws applicable in Uganda for cybercrimes are The Computer Misuse Act, No. 2 of 2011. This Act regulates cybercrime to promote the safety and security of electronic transactions and information systems; prevents unlawful access, abuse, and misuse of electronic devices like mobile phones including computers, and secures the conduct of electronic transactions in a trustworthy electronic environment in addition to providing for other related matters The Ugandan Parliament has passed the Computer Misuse (Amendment) Bill, 2022 which prescribes tougher penalties for those perpetrating cyber-crimes. Among the regulations in the law is a provision barring the sharing of information relating to a child without the consent of a parent or guardian. The bill also seeks to prohibit the sending or sharing of information that promotes hate speech as well as unauthorized access to information or data.[144] Another legislation providing for cybercrimes and cybersecurity is The Electronic Signatures Act - regulates the use of transaction signatures and ensures that transactions are carried out in a secure environment; enhances authenticity and security of documents by establishing a public key infrastructure.[145] The Electronic Transaction Act - provides for the use, security, facilitation, and regulation of electronic communications and transactions is another legislation providing for cybercrimes provisions.[146]

Despite presence on laws in force as addressed in this part in respect of Uganda, no any of the law provides for specific provisions relating mutual legal assistance procedure to cybercrime investigation or otherwise.

iii. Burundi

Generally, there is no specific legislation to criminalize unlawful cybercrimes. however, under Law No 1/09 of May 11, 2018, assented by Burundi's president, which amends the Code of Criminal Procedure of 2013. There are also legislations that do provide for several offenses, policies, and acts in relation to cybercrime, [147] The Constitution of Burundi of 2018 contains provisions on the privacy of communication, and regulation of evidence collection according to art. 47 government agencies carrying out investigations can intercept electronic communications and seize computer data, The Penal Code Act, No. 1/95 of 22 April 2009 has provisions on electronic transactions. On 29 April 2009, Burundi adopted a new Penal Code which took into account the new criminal phenomenon of cybercrime. The specific legislation on cybercrime is – art. 467-470 (forgery, fraud, illegal access, and system interference).[148]

The laws above have no provision relating mutual legal assistance procedure to cybercrime investigation or otherwise. The Acts above have only provided for national procedure and protection of cybercrime.

iv. Rwanda

Rwanda maintains two sets of laws addressing cybercrimes. The laws applicable in Rwanda on cybercrime matters are, Law No. 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes (Law on Prevention and Punishment of Cyber Crimes of 2018)[149] and Law No. 24/2016 governing

[143] https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/kenya.
[144] https://www.academia.edu/3630851/INFORMATION_TECHNOLOGY_LAW_AND_CYBER_CRIME_IN_UGANDA.
[145] Ibid.
[146] Ibid.
[147] https://www.coe.int/en/web/octopus/-/burundi.
[148] https://core.ac.uk/download/pdf/33424823.pdf.
[149] https://www.coe.int/en/web/octopus/-/rwan-1.

Information and Communication Technologies – Establishes a framework for ICT policy and regulation, with emphasis including on: promoting national ICT policy objectives; establishing a licensing and regulatory framework in support of national policy objectives for the ICT industry; Comprises a section on matters of national interest and data security,[150] including provisions on interception and monitoring of information, privacy and data protection, powers of the Minister on issues of national sovereignty, disaster management plans.[151]

Again, just like other state of affairs in the EAC, the laws above have no provision relating mutual legal assistance procedure to cybercrime investigation or otherwise. The Acts above have only provided for national procedure and protection of cybercrime.

10. Conclusion and recommendations

The study, with regards to the status of legislation on general mutual legal assistance in combating cybercrimes within the EAC, has revealed that each of the selected EAC member state maintain certain procedures governing mutual legal assistance in criminal matters but not specific to cybercrimes. At least every country has in place the regulations enabling the requesting states to request for the assistance and the requested state to cooperate and respond accordingly.

In relation to the status of cooperation in investigating, prosecuting, and punishing cybercriminals in the EAC, the study revealed that the status of cooperation in investigating, prosecuting and punishing cybercriminal in the EAC is not convincing. The reason for this being the fact that there are no specific binding laws prescribing the manner in which the member states of the EAC are supposed to support each other where the need arises.

On need for comprehensive, harmonised, and practical framework on mutual legal assistance to combat cybercrimes in the EAC Member States, the study revealed that EAC needs to harmonise its laws on the account that each country has its own laws but that which are not specific to the cybercrimes. The harmonisation of laws needs also to take into consideration the practicality of the laws governing mutual assistance in view of the nature of cybercrimes.

Given the above conclusions, the following are the recommendations based on the nature of the problem studied.

i. Compliance with the EAC Treaty

It is evidence that spirit for having in place a common mutual legal assistance within EAC was crafted at the inception of drafting a treaty. Article 124(5) of the Treaty is specific on the provisions regarding mutual assistance in criminal matters. In particular, Article 124(5) provides that:

The Partner States agree to enhance co-operation in the handling of cross border crime, provision of mutual assistance in criminal matters including the arrest and repatriation of fugitive offenders and the exchange of information on national mechanisms for combating criminal activities. To this end the Partner States undertake to adopt the following measures for maintaining and promoting security in their territories to:

(a) Enhance the exchange of criminal intelligence and other security information between the Partner States' central criminal intelligence information centres;

(b) Enhance joint operations such as hot pursuit of criminals and joint patrols to promote border security;

[150] Section 7 of the Act.
[151] (Octopus Cybercrime Community, 2023).

(c) Establish common communication facilities for border security;
(d) Adopt the United Nations model law on mutual assistance on criminal matters;
(e) Conclude a Protocol on Combating Illicit Drug Trafficking;
(f) Enhance the exchange of visits by security authorities;
(g) Exchange training programmes for security personnel; and
(h) Establish common mechanisms for the management of refugees.[152]

This provision needs to be implemented by the EAC member states. Through this provision, the treaty sets the basis for the cooperation which the member states must use to harmonise laws in fighting against cybercrimes. For practical and best approach, it is recommended that EAC member states adopt in place a single legal instrument whereas major factors for cooperation will be depicted, principal agreement in respect of dual criminality will be addressed and as well areas for cooperation.

ii. Designation of Cyber Security Offices

In combating cybercrimes, high skilled personnel with information and communication technology cannot be underrated. As cybercriminals invoke the use of high technology in committing crimes, the investigation machinery in collaboration with prosecution machinery need to have as equal or relatively high IT experts who will counter the cyber threats and fight the cyber criminals. Learning from the best practice of members of The Budapest Convention where there are offices dealing with cybercrimes, establishment of cyber security offices with proper communication duly authorized by relevant laws to arrest, block, collect evidence and preservation of the same, the rate of cybercrimes shall be reduced. Unlike traditional crimes, cybercrimes need fast response to the reported events thus necessitating abolition of hard, time consuming and complicated method of conducting mutual legal assistance.

iii. Bilateral Agreements

As stated, some members of EAC have no in place bilateral agreements to combat traditional crimes through mutual legal assistance. The situation becomes worse as regard to cybercrimes because of the nature of the cybercrimes and its implications as a whole. Presence of bilateral agreements which shall specially address the aspect of mutual legal assistance in criminal matters shall assist in combating the high rate of cybercrimes. Absence of even mutual legal assistance in traditional crimes makes it difficult for relevant authorities to combat cybercrimes.

iv. Establishing Areas of Cooperation

As it is in principal that cooperation through mutual legal assistance requires to be in agreement as to what offences to be incorporated in cooperation, each EAC member states should depict what acts, omission or abstinences constitutes cybercrimes for the purpose of mutual legal assistance. That is imperative as the principal of dual criminality entails that both parties to the agreement criminalize the acts agreed for the purpose of mutual legal assistance. Absence of such consensus compromises the entire rationale for mutual legal assistance.

v. Proactivity of the Laws

Though the court is praised for its effort in making sure that some of the EAC member states keep pace with the technological advancement,[153]there should not be an over reliance on judicial pronouncements or waiting until judges settle the matter by introducing judicial rules which sometimes are untimely.[154]

[152] East African Community, The Treaty for the Establishment of the East African Community, Arusha. EAC: 2002 xiv, 111p.: 230mm (EAC Publication, No.1).
[153] See, *Tanzania Cotton Marketing Board v. Cogecot Cotton Company SA* [1997] TLR 165 (CA) and *Trust Bank Tanzania Ltd v. Le-marsh Enterprises, Joseph Mbui Magari, and Lawrence Macharia*, The High Court of Tanzania (Commercial Division) at Dar es Salaam, Commercial Case No.4 of 2000 (Unreported).

vi. Reformation of Legislations

Based on the findings, the reformation of the legislations in all EAC member states in relation to mutual assistance in criminal matters is recommended to embrace technological advancement which challenges the use of traditional methods of sending and auctioning requests for assistances from the requested states. As Karl Max contends, laws should respond to the stimulus of social economic changes. It is important to note that laws should change in order to match with the requirement and demand of the society. Since laws are enacted for the welfare of the people, changes to the social structure and living should have impact on them. It does not mean that the laws are to be changed for the sake of changes, but they are to always reflect the nature and profile of the society where they are applicable.

vii. Capacity Building

Mutual legal assistance in relation to cybercrimes require a high-level of expertise because technology keeps on changing and becomes so complex day by day. Training is needed to address the knowledge gap and expertise among Judges, Magistrates, prosecution machineries and other officers involved in the entire chain of mutual assistance in cybercrimes. In addition, it is recommended that guidelines be designed and training programs developed for all stakeholders to understand how best to strengthen the mutual assistance in digital environment.

As stated in chapter two, the law enforcement agencies (Judiciary, TPF and DPP) possess inadequate capacity in cybercrime investigation and prosecution. Though the Judiciary and DPP have extensive knowledge on prosecution of crimes, they lack some capacity in tackling cybercrimes. There is currently limited capacity of judges across the country in presiding over cases relating to cybercrimes, or crimes requiring the use of electronic evidence as well.

African Union Cyber Security Experts Group (AUCSEG) under the auspices of the African Union Commission (AUC) admits that capacity development related to improving people, process and technology and related strategies of enhancing evidence sharing, judicial cooperation and assistance in criminal investigations and prosecutions that involve possible cybercrimes is imperative. The Experts Group also reiterated the need for the improved and streamlined law enforcement's ability, in various jurisdictions, to obtain and exchange evidence needed for investigations and prosecutions and deepen the cooperation against terrorism and transnational organized crime, including cybercrime. Technical assistance support on infrastructure development for developing countries e.g., Computer Emergency Response Teams (CERTs) was also capitalised.[155]

viii. Learning from Best Practice

The collaboration in the fight against cybercrimes in EU countries is strong compared to East African countries. On that basis, the EAC member states can develop their mechanisms of perfecting mutual assistance in cybercrimes by adopting the best practices from the European countries or by using the model laws which are otherwise not binding if not adopted as such.

ix. Judicial Activism

The court is said to be proactive when it sets or adjudge cases on basis of personal inclinations. The decisions are far beyond the correlations of the law. Generally, judicial activism is devised where the law has not addressed the matter at the hand of the decision makers. Where laws are made to be

[154]Lukumay, Z. (2011) *Electronic Banking: It's Legal Basis in Tanzania*, Deutschland: Lambert Academic Publishers, p.306.
[155] Responses to Guiding Questions input into the UN AdHoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Third Session, New York, 29 August – 09 September 2022 accessed through African_Union_AHC3.pdf (unodc.org) on 29 September 2023.

proactive to changes, judicial activism in many states shrinks. In Tanzania, the development of information and communication technology in judicial context was not firstly covered by the proactive nature of the laws. History entails that, courts started to spearhead the invocation of technological development in the judicial context most especially in relation to the reception of the electronic evidence.[156]

Laws were enacted as a heed to the judicial call. The case of Tanzania Cotton Marketing Board v. Cogecot Cotton Company SA.,[157]started to demonstrate the activeness of judiciary in absence of the law. This happened after it acknowledged the use of electronic communication as a medium through which an arbitral award may be sent. The acknowledgment was, by then, inconsistent with the Arbitration Act,[158] the law. Owing to its peculiarity, the case influenced the decision of the court in the remarkable case of Trust Bank Tanzania Ltd v. Le-marsh Enterprises, Joseph Mbui Magari, and Lawrence Macharia.[159] The latter, has grounded the foundation of peripheral laws in administration of justice in the technological era labored. To be exact, the mentioned cases were with bias to the admissibility of the electronic evidence. In Lazarius Mrisho Mafie & Another v. Odilo Gasper (supra), the trend went on where, relevancy of the electronic evidence to be admitted, its authenticity, best evidence rule, rule against hearsay, and probative value of the evidence intended to be tendered, were mentioned as sine quo non for the reception of electronic evidence. This initiative can also be used in relation to the need for the collaboration among EAC member states to be strengthened in the fight against cybercrimes which is on increase as a result of technological advancement.

REFERENCES

Books

1. Bailey, E.C, Counterterrorism Law and Practice in the East African Community, Brill Nijhoff, Boston, 2019.
2. Council of Europe, Mutual Legal Assistance Manual, Council of Europe, Belgrade, 2013.
3. Hoercke, M.V and Ost, F, Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline? Hart Publishing Ltd, Oxford, 2011.
4. Mwiburi, A.J and Majamba, H. I, "Overview and Methodological Approach in Harmonizing Cybercrimes Law in East Africa" in Mwiburi, A.J and Majamba, H. I, Harmonization of Cybercrimes Legal Frameworks within the East African Community, University of Dar es Salaam School of Law, Dar es Salaam, 2020.
5. United Nations Office on Drugs and Crimes, Manual on Mutual Legal Assistance and Extradition, United Nations Office, Vienna, 2012.
6. Verdelho P, The Effectiveness of International Co-operation against Cybercrime: Examples of Good Practice, Economic Crime Division Directorate General of Human Rights and Legal Affairs Strasbourg, France, 2008.
7. **Articles**

[156]Mambi, A. (2009) "A Decade after the Establishment of the Commercial Court Division: The Role of the Court on the Legal Changes Towards the Use of ICT (Electronic Evidence) in the Administration of Justice in Tanzania" *Tanzania Lawyer Journal*, Vol. 3, Issue No. 2,pp.121-137, p.127.
[157][1997] TLR 165 (CA).
[158] [Cap 15 R.E 2002].
[159][2002] TLR 144.

8. Cassim, F, 'Addressing the Growing Spectre of Cybercrime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players, Addressing the Growing Spectre of Cybercrime in Africa', XLIV CILSA 2011.
9. De Busser, E.D, 'The Digital Unfitness of Mutual Legal Assistance', Security and Human Rights Journal, 2017, Vol.28, pp.161-179.
10. David, D & Luca, G, 'Do Police Crackdowns Disrupt Drug Crytomarkerts? A Longitudinal Analysis of the Effects of Operation Onymous' Crime, Law and Social Change, 2017, Vol. 67, Issue No. (1), pp. 55-75.
11. Mitchell J., 'Africa Faces Huge Cybercrime Threat as the Pace of Digitalisation Increases', The Investment Monitor, 16 June 2022.
12. Orji, U. J, 'The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?' Masaryk University Journal of Law and Technology, Vol.12, Issue No.2, pp.91-129.
13. Osula, A, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data', Masaryk University Journal of Law and Technology, Vol.9, Issue No.1, pp.43-64.
14. Tamarkin, E, 'The AU's Cybercrime Response: A Positive Start, but Substantial Challenges Ahead', Policy Brief 73, January 2015, Institute for Security Studies.
15. Jason Mitchell, Africa FaceIMPER **Reports**
16. Kennedy G., Relevance of International Law in Combating Cybercrimes: Current Issues and AALCO's Approach, Presentation at the 4th World Internet Conference, Wuzhen Summit, on the Session on International Cooperation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes", 4th December 2017, Wuzhen, China.
17. Mwaita, P & Owor M., Workshop Report on Effective Cybercrime Legislation in Eastern Africa, Dar es Salaam, Tanzania, 22 August 22-24, 2013.
18. Rees A., International Cooperation in Cybercrime Investigations, Computer Crime & Intellectual Property Section Criminal Division, U.S. Department of Justice. OAS Regional Cyber Crime Workshop, April 2007.

Online Sources

1. www.unodc.org
2. https://www.vertic.org/media/National%20Legislation/Montenegro/ME_Law_Mutual_Legal_Assistance.pdf
3. Https://Au.Int/En/Treaties/African-Union-Convention-Cyber-Security-And-Personal-Data-Protection
4. https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240
5. https://www.ccdcoe.org/uploads/2010/07/Legal_Cooperation_to_Investigate_Cyber_Incidents_Estonian_Case_Study-and_Lessons.pdf
6. https://www.ccdcoe.org/uploads/2010/07/Legal_Cooperation_to_Investigate_Cyber_Incidents_Estonian_Case_Study-and_Lessons.pdf
7. https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdff
8. https://law.indiana.libguides.com/dissertationguide
9. https://rm.coe.int/1680081561

10. https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-7-Cybercrimes.pdf
11. https://landportal.org/book/narratives/2022/tanzania
12. https://fbattorneys.co.tz/cyber-attacks-how-the-tanzanian-laws-protect-us/
13. https://www.eac.int
14. https://www.minijust.gov.rw/news-detail/law-enforcement-agencies-must-step-up-by-enhancing-measures-to-detect-and-prevent-the-cyber-attacks-from-the-source
15. https://allafrica.com/stories/202207190053.html
16. https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/
17. https://www.burunditimes.com/burundi-passes-tough-law-on-cybercrime
18. https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter
19. https://www.oecd.org/digital/ieconomy/2494779.pdf
20. https://www.oecd.org/digital/ieconomy/2494779.pdf
21. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection https://au.int/en/recs/comesa#:~:text=The%20PTA%20Treaty%20envisaged%20its,Malawi%20on%208th%20December%201994
22. https://www.comesa.int/wp-content/uploads/2020/05/2011Gazette-Vol.-16.pdf
23. https://www.sadc.int/member-states
24. https://www.sadc.int/
25. https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf
26. https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/cybersecurity-cybercrime-africa-continentalregionalpolicies/#:~:text=Out%20of%2055%20AU%20members,(as%20of%20March%202022).&text=Countries%20that%20have%20ratified%20the,%2C%20Senegal%2C%20Togo%2C%20Zambia.
27. https://www.eac.int/eac-history
28. https://statelaw.go.ke/wp-content/uploads/2020/11/MLA-GUIDELINES-IN-CRIMINAL-MATTERS-FOR-AUTHORITIES-OUTSIDE-OF-KENYA.pdf
29. https://ungreatlakes.unmissions.org/sites/default/files/uganda.pdf
30. https://www.unodc.org/pdf/lap_mlaeg_report_final.pdf
31. https://fbattorneys.co.tz/cyber-attacks-how-the-tanzanian-laws-protect-us/
32. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/kenya
33. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/kenya
34. https://www.academia.edu/3630851/INFORMATION_TECHNOLOGY_LAW_AND_CYBER_CRIME_IN_UGANDA
35. https://www.coe.int/en/web/octopus/-/burundi
36. https://core.ac.uk/download/pdf/33424823.pdf
37. https://www.coe.int/en/web/octopus/-/rwan-1