RUAHA CATHOLIC UNIVERSITY

FACULTY OF LAW

Critical analysis on cyber crime prevention and protection by Tanzania police force: cyber mobile bullying

A Research Paper Submitted in Partial Fulfillment of the Requirements to Awards of the Bachelor of Laws (LL.B) Degree of Ruaha Catholic University

By:

NDIMBO HERBERT

Reg no. No. 408/LLB/T/2015

Prepared Under supervision of

Ms: ELIZABETH LUKELELWA

JULY 2019

CERTIFICATION

The undersigned, certifies that she has read the entire work and hereby recommends for acceptance by The Ruaha Catholic University dissertation titled “Critical analysis on cyber crime prevention and protection by Tanzania Police Force: Cyber mobile bullying.”, in partial fulfillment of the requirements for the Bachelor of laws degree (LLB) of Ruaha Catholic University.

.....

Ms: ELIZ**A**BETH LUKELWA

(Supervisor)

.....

Date

COPYRIGHT

This dissertation is a copyright material protected under the Berne Convention, the Copyright and Neighboring Rights Act, [R.E 2002] and other international and national instruments in that behalf, on intellectual property. It may not be reproduced by any means, in full or part, except for short extracts in fair dealing, for research or private study, critical scholarly review or discourse with acknowledgment, without written permission of both the author and the Ruaha Catholic University.

DECLARATION

I, Ndimbo Herbert, do hereby declare that, this Dissertation is my own work and that it has never been submitted anywhere by any person in either a whole or part of it for the Bachelor degree in law or in any other field or award related to this.

.....

Signature

.....

Date

DEDICATION

This entire work is dedicated to my family with specific attention to my beloved parents Mr and Mrs Ndimbo.

I would like also to thank Mr. Sumleki Mamboleo, Mgina Dickson, Mariam Mageta, Patrick Steven, all Classmates and Police officers from the most senior to most junior for their support and assistance in my academic life.

TABLE OF CONTENTS

STATUTES

International Legal Instruments

Extradition Act 41

International Telecommunication Union

Budapest Convention on Cyber Crimes, 2001.

Domestic legal Instruments

The Constitution of United Republic of Tanzania of 1977

Cyber Crimes Act, 2015 and the Electronic Transactions Act, 2015

The electronic and Postal Communications Act (EPOCA)

The Penal Code44

ABSTRACT

The recent development of information and communication technology (ICT) has led to increase of different forms of cybercrimes. These forms of cyber crimes have become the major threat of individual, such developments pose many challenges to the administration of criminal justice, affecting particularly the whole process of investigation and prosecution of crimes in Tanzania and in the world at large.

The aim of this study is to examine the critics towards prevention in the process of investigation prosecution of cybercrimes by police Force. In doing so, the study examines the existing laws and practices in Tanzania. The study draws a survey from the legal, economic and social perspective on various challenges that are associated with the investigation of cyber crimes. This research has four chapters whereby the first chapter provide for general introduction. Chapter two structured the Legal framework on cybercrime. Chapter three provides critical analysis of the Cybercrime Prevention, Protection and Prosecution by Police Force and Last chapter provide for conclusion and recommendations.

CHAPTER: ONE

GENERAL INTRODUCTION

1.1Background of the problem

According to Michael (2005) the term crime has been derived from the Latin word "crimen" which means charge, indictment, accusation, fault or offence, then in late 14th century the term started being used to refer offence punishable by the law, according to Oxford English Dictionary crime is an act or omission which constitute an offence and is prohibited/punishable by law, such an act should be which is unlawful[1].

The revolt in information technologies (ICT) in 21st century has changed society fundamentally and will probably continue to do so in the foreseeable future. Many tasks have become easier to handle[2]. Where originally only some specific sectors of society had rationalized their working procedures with the help of information technology, now hardly any sector of society has remained unaffected. Information technology has in one way or the other pervaded almost every aspect of human activities

These developments have given rise to unprecedented economic and social changes, but they also have a shadowy side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Technical measures to protect computer

[1] AJ. Mambi, ICT Law book: A Source Book for Information & Communication Technologies and Cyber Law, Mkuki na Nyota, Dar es salaam 2012, 89.

[2] H.T.Tavani, Ethics and Technology, 2nd Ed, John Wiley & Sons Inc, USA 2010, 67

systems and other communication tools need to be implemented concomitantly with legal measures to prevent and deter criminal behavior**.** [3]

This research design is to provide an intensive framework on how the research is going to be carried out, and the reasons as to why it should be conducted. Particular on the critics facing Police Force while investigating and prosecution of cyber crimes and causing delay of proceeding in Tanzania, Iringa Region as a case study. The discussion is made on, background of the problem, statement of the problem, Aims and objectives of the study, significance of the study, hypothesis, literature review, research methodology, method of data collection, data analysis, and scope of the study and limitation of the study.

1.2. Statement of the Problem

The United republic of Tanzania Government has a goal of reducing eliminating crimes in the country. With this regard it has encouraged the prevention of crimes through various ways. There are several steps/measures taken by the government using police Force Cyber Crime Unit so as to prevent crimes such as cyber bullying, stealing of money from banks and mobile example Mpesa, Tigo pesa, Airtell Money etc.

Despite the government effort of preventing crime especially cyber crimes by use of Police Force Cyber Crime Unit it seems that there is problem on proceeding aspect of dispending justice to an accused person of cyber crime at court proceeding, the proceeding require the enough proof and evidence beyond the reasonable doubt for the person to be found guilty of an offence charged with. Proceeding do require that if the person is convicted of cyber crime example those cyber crime relating to stealing through mobile phone network (Mpesa) then the record and any

[3] Conventions.coe.int/treaty/EN/Reports/html/185.htm. Accessed, 2/1/2019

relevance evidence could only be obtained from the head quarter. The process of bringing the Legal Officer or Advocate of the company might take time and cause unduly delays of proceeding. Justices delayed justices denied

The constitution of United Republic of Tanzania of 1977 and other laws of the land provide for the right of fair and speed trial of the case[4], and this is one of the important pillars in relation to rule of law. That justice should be done to all equally and court should resolve matters before them within the reasonable time and without unduly delay.

Article 107A(2) provide as follows in delivering decision in matters of civil and criminal in nature in accordance with the laws, the court shall observe the following principles, that is to say[5]Impartiality to all without due regard to ones social or economic status and not to delay dispensation of justice without reasonable ground.

This predisposed the researcher to conduct this research in order to examine and to understand whether these delays are either caused by lack of sufficient evidence or rules and procedure governing Criminal police investigators hinders them to conduct investigation of cybercrimes.

1.3.0. Objectives of the Study

1.3.1 General Objective

The general objective of this study is to critical analysis and examine the challenges facing criminal investigators and prosecutors in dealing with Cyber Crimes which lead to delay of dispensation of justices; to provide for attribute for the developing appropriate legal framework

[4] A, Makulilo., (2011) Registration of SIM cards in Tanzania: a critical evaluation of the electronic and postal communications Act, 2010. Computer and Telecommunications Law Review.
[5] The Constitution of United Republic of Tanzania of 1977.

which will enable CID's and DPP to carry out their duties effectively to case relating cyber stilling on mobile phone networks.

1.3.2. Specific Objectives

The research aims at achieving specifically the following objectives:-

To examine the laws which are governing cyber bulling in Tanzania and evaluate proceedings of resolving cyber bulling cases

To determine the extent to which the current legal framework addresses the challenges brought by the development of ICT and its related challenges;

1.4. Significance of the study

The research will help the researcher to obtain his LLB.

Secondly the research will help law makers to make up their minds on cyber bullying offences and how insure cases are determined without delay.

Thirdly the results will help the community to change their attitude against the Government and to enable the police force to enhance, perform the investigations functions according to law so as to adhere the principle of natural justice in relation to the changes of science and modern technology.

1.5 Literature Review

This part basically entails different literature pertaining to cyber crimes which are the subject matter of the research.

Paula Musuva-Kigenc[6] Mobile money in Tanzania has experienced numerous attacks through social engineering, use of malware and account impersonifications. As one of the alternative channels for most banks, hackers are now exploiting the weak security controls around the mobile money platform to steal millions of dollars. Mobile Money Services

Majority of banks, merchants and service industry firms in Tanzania are now adopting mobile money services to serve as one of their alternative channels. Mobile money is integrated into the other sectors including hospitality, banking, transportation, telecommunication, E-commerce, government and other financial sectors. With that growth come a whole new set of threats: mobile malware, third-party apps, unsecured Wi-Fi networks, risky consumer behavior. It does not matter whether an institution uses a proprietary or third-party mobile banking application – they still own the risks. In recent times, hackers have exploited the weak security controls around the mobile money platform to steal millions of dollars especially from banks.

Ozeren, Suleyman[7] in his study *Global response to cyber terrorism and cybercrime: A matrix for International cooperation and vulnerability assessment*, he describe that Cyber terrorism and cybercrime present new challenges for law enforcement and policy makers. Due to its transnational nature, a real and sound response to such threat requires international cooperation involving participation of all concerned parties in the international community. However,

[6] Serianu Cyber Threat Intelligence Team in partnership with the USIU's Centre for Informatics Research and Innovation (CIRI), at the School of Science and Technology.

[7] Ozeren, Suleyman, Global response to cyber terrorism and cybercrime: A matrix for International cooperation assessment,digital.library.unt.edu/ark:/67531/metadc4847/m2/.../dissertation.pdf (accesses 25th February 2019).

vulnerability emerges from increased reliance on technology, lack of legal measures and lack of cooperation at the national and international level represents real obstacle toward effective response to these threats. Terrorist and cyber criminals will exploit vulnerabilities, including technical, legal, political and cultural. Orezen study, identified variables that constructed the scale based on the expert opinion. Also, the study presented typology of cyber terrorism, which involves three general classification of cyber terrorism Disruptive and destructive information attacks, facilitation of technology to support ideology and communication, fund raising, recruitment.

Mr. Adam Mambi[8]; views cyber security issue from legal perspective; the author argues that legal framework is an essential aspect for a sustainable cyber security. The premise from this is that as ICT becomes perverse, knowledge and skills advance, traditional and new skills committed are also in increase. Such a situation requires a comprehensive legal environment to ensure that crimes are understood and accommodated through laws, policies, regulations, and guidelines. The legal environment in Tanzania is still inadequate for cyber security in the country. This is because the existing laws were developed before the development of computer technology. The laws were made to facilitate the traditional paper based business environment. This situation poses a serious challenge to Tanzania to accommodate modern cybercrimes such as fraud, theft of data, laundering, transmission of harmful codes, unauthorized access to information, impersonation, etc. The Government of Tanzania is aware of the inadequacy of the legal framework for cyber security in the country. Accordingly, in 2007, the Government amended the Evidence Act to accommodate the validity of electronic evidences. Further, the Electronic and Postal Communication Act, 2010 (EPOCA) is in place. Tanzania needs to fast

[8] Cybercrimes Act, 2015

track the development and enactment of a comprehensive legal framework to ensure a safer cyber Tanzania. This can be achieved by (1) adopting an effective legal framework to combat cybercrime and other misuses of information technology, (2) enact enforceable cyber laws in a well-defined geographical boundaries that are either national or regional, (3) fostering international cooperation, information sharing, and investigative assistance. The author did not provide the manner and proceeding in relation to the obtaining the information or evidences for the purpose of the investigation where it's the major problem lead the researcher to conduct this research.

Dr. Amos Nungu[9]; in his paper, he outlined two major things. Firstly is that the government has the role and duty of ensuring that there is an adequate legal and practice environment (policies, laws, standards, regulations are available and enforcement mechanism) to allow secure and safe cyber transaction. And secondly, the industry must implement and comply with the international and contextual legal frameworks and industry standards to create for secure digital operations.

Lilians Edwards and Charlotte Waelde [10] jointly explored on the issues policing the Internet, discussion on challenge facing police investigator in investigation of cyber crimes. It will be argued that the study is indeed in Tanzania situation because the subject matter is universal. However the Authors failed to analyze the legal issues if the law in place is conducive to allow effective investigation of cyber crimes which might be one of the legal setbacks in investigation of these crimes. Authors also did not address the challenge as per Tanzania context

Anthony and Kevin[11] stated and addressed challenges involved in the computer related incidents. They pinpoint challenges that police investigators face in the process of investigation

---

[9] 2000
[10] Lilian Edwards & Chalotte Waelde, Law and the Internet, 3rd ed.(united state: Hart Publishers, 2009) 608-609
[11] Anthony Reyes & Kevin O'shes , Cyber Crime Investigation2nd ed (New York: Hart Publishers, 2007)2-7

to be the gaps in the cyber law. An investigator finds posting hypothetical question, which in most of the time the evidence collected will never be admissible.

They also argued that the investigation of cybercrimes can be very intimidating to technophobe, many police, prosecutor, when you report to them that you had crime that involves computer many of expression would transform to unwelcoming look. The work of these Authors is very important as they pinpointed challenges.

Robert Moore[12] in his book he pinpointed challenges on investigation of cybercrimes and technique to conduct investigation on computer related crimes, this includes jurisdiction which he stated that it is very difficult to determine who has the authority to investigate high-technology crime, However the Author spend much of book particular on the techniques to conduct investigation rather than the major challenges facing investigators in investigating cyber crimes.

Ian J. Lloyd[13] portrayed challenges on detecting and prosecuting computer crime, such as the identity of the wrong dower and obtaining sufficient evidence to support criminal conviction.

Janine and Ronnie[14] stated on government Investigatory Powers in investigating cyber crimes whereby they argued that the U.S federal government believes that it needs effective tools in the fight against cyber crimes same of these tools that the government would like to use are controversial and may conflict with fundamental policies of privacy. Their work is very important because it states on how investigation may be limited in order to ensure person's privacy. However right of privacy may be a setback to investigation.

---

[12] Robert Moore, Cyber Crime investigation 2nd E.d (Elsevier Inc, 2011)5
[13] Ian J. Llyoid, Information technology law 6th ed.(Newyork: Oxford university Press, 2010)262
[14] Janine S.Hiller & Ronnie Cohen, Internet Law and Policy 1st ed.(New Jersey: Pearson Education Inc, 2002)165

As per Tanzania jurisdiction few literature were obtain by the researcher, and these can be explained as follow.

Mollel and Lukumay[15] portrayed the challenges associated to Electronics evidence that they pinpoint that electronic evidence is very temporary in nature of digital data .it is very easy to view, copy ,modify or destroy digital record; be in a number , document or image .Although digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combination, the combination of high percentage of fraud with employee involvement and the possibility that raw data can be modified by an individual with immediate access to the system means that any evidence collected from the system has a questionable and unverifiable level of integrity. In such circumstances the police officer may not get proper records in relation to electronic evidence.

The study of these Authors is very significant because during the investigation of cyber crimes the police officer will have to collect evidence which will be electronic in nature , and has pointed out by the authors the best evidence rule is applied to ensure reliability that is to say integrity, of the documents or records. However the researcher find this research topic still researchable because the Authors were limited to how the law of evidence has an impact to electronic evidence and not the general challenge from legal, social and economic perspective that faces the police officers in investigating cyber crimes.

Adam J. Mambi[16] portrayed the legal challenge of Electronic crimes and difficulties of investigation and prosecution cybercrimes. He further analyzed how jurisdiction is a problem to

[15] Andrew Mollel & Zakayo Lukumay, Electronic Transaction and Law of Evidence in Tanzania, (Paramiho: Iringa University College, 2007) 78

[16] Adam J. Mambi, Information and Communication Technologies and Cyber Law, 1st ed (Dar-es-salaam:Mkuki na Nyota Publishers 2010, 97.

the law enforcement agencies. He also pinpoints the problem that might arise due to nature of borderless of e-crimes that they may cause difficult in identification of parties, laws or judicial rules of evidence that should be applied and how can the deleted files be covered.

However researcher was limited on how jurisdiction posses challenges in investigation of crimes and not on prosecution this is why the researcher finds this research important to research about.

Queen[17]; The rationale for speedy process is to safeguard the interest of the accused on the one hand and of the victims of the crimes and the community on the other.

Most legal systems presume that accused persons are innocent until they are proved guilty. Hence the first rationale for the speedy process is to reduce the period between the arrest of the accused persons in connection with the cyber crime offences and the conclusion of the trials. Most of the case law and literature express concern about pre-trials incanceration. The fact is however that in many systems there is more or less the same magnitude incanceration between the commencement and conclusion of trials. The second rationale is therefore to minimise the pain, anxiety concern[18] and uncertainty[19] on the part of the accused that normally go with prolonged incarceration. The third rationale is that, the defence of the accused may be impaired due to the lapse of memory following a long period of waiting for the trial. Loss of memory also applies to witnesses whom the accused may intend to call in his defence[20]. In addition the witness may not be available at the time of trials for a number of reasons from simple change of

---

[17] (1978),33 CCC(3d) 289,57 CR(3d)289.

[18] Barker v. Wingo 407 US 514 (1972).

[19] Stogmuller v. Austria (1979-80),EHRR 155.

[20] R. v. Mingati and Others.

address to death[21]. Moreover vital exhibits may also be destroyed in the process of waiting for the trials. The combination of these factors may easily occasion a miscarriage of justice.

All victims of cyber crime offences are for different reasons similarly anxious to see the conclusion of their cases. Thus the first rationale is to see that justice is done by ensuring that all material evidence is submitted before the court delays in the conclusion of trials,

All victims of criminal offences are for different reasons similarly anxious to see the conclusion of their cases. Thus the first rationale is to see that justice is done by ensuring that all material evidence is submitted before the court delays in the conclusion of trials, cyber crime cases included. Perhaps worse of all there may be the fear that the accused will take advantage of absence of such evidence to secure acquittal.

Over and above all, it is the general interest of the society to see that the guilty are punished and the innocent are exonerated. There is concern that delays in criminal process may allow the accused to manipulate the system or commit further offence. But caution must be exercised on excessive speed. Discussing the balance of interest between the prosecuting state and accused, the European Court of Human Rights has observed that the right of examination of a case with expedience must not hinder courts to carrying out their tasks with the due cases. Furthermore, the Human Rights Committee has cautioned that extra speed may, in certain cases, contribute to the failure of justice[22].

---

[21] Martzneller v.Austria (1979-80)1 EHRR 98 Para 2(c); Wemhoff v. Republic of Germany (1979-80); Neumeister v. Austria (1979-80)EHRR 91 Para 4(2)

[22] This includes instances where accused may be acquitted because of poor investigation and preparation of prosecution case in order to dispose it quickly. Unfortunately this brings us back to the controversial issue of what constitute reasonable speed in varying circumstances.

1.6 Hypothesis

It appears that the laws that governing cyber crime particularly cyber bullying to mobile phones is not adequate enough to combat the problem.

1.7 Research Methodology

The research compiled both field research and Library research.

1.7.1 Field Research

A combination of methodological tools has been used in this research based on the qualitative strategy to collect relevant data. These are review of literature which will be conducted at the Ruaha Catholic University , and the field (survey method) which will be conducted in the Iringa Police Station especial to the Cyber crime Department Resident Courts, Director of Public Prosecution Office, and in the office of Director of Criminal Investigation Department, also interviews will be used in order to seek opinions from various individuals whom the researcher thought might have knowledge on various issues related to criminal investigation and prosecution of cyber crimes.

The researcher interviewed 40 respondents in which 15 were from the Police station Cyber crime unit department, 15 others were from the prosecution offices and the remaining 10 were from the Court.

The researcher focused to certain group of person who were relative and aware to the whole matter relating to the cybercrime offence and situation of it in Tanzania.

1.7.2 Library Research

Various sources have therefore been used by the researcher to obtain these types of data, researcher with not only texts books, journals and various reports but also unreported cases that were suitable to this study. These methods of data collection will involve sources like books, journals, articles and websites from library. This enabled the researcher to understand how the previous authors dealt with cybercrimes investigation, and by so doing the researcher will be in the better position to fill the gap which are not covered in relation to the current situation of science and technology.

1.8. Scope and limitations of the study.

1.8.1. Scope of the study

The scope of the study is on the challenges facing police investigator and state attorneys in investigation and prosecution of cyber crimes especially Mobile Money Services crime and causing delay of dispensing of justices the area of the study is Iringa Region were data shall be collected regarding to the concerned topic. The researcher intends to visit police station,

1.8.2. Limitations of the study.

The researcher encountered number of limitation in the process of data collection. Firstly the Staff criminal investigation departments in Iringa Municipality were to some extent not ready to give comprehensive data in relation to the study because they were not stored anywhere due to lack of ICT knowledge hence poor record keeping. Secondly the researcher could not get full cooperation from the mobile phones companies such as Tigo, Airtel and vodacom and banks companies on the ground that such information is confidential for the interest of the company

business and duty to secrecy towards their clients, Also the researcher faced financial constraints the conduct such research would require the larger amount of cash for the accomplishment of research lastly time shortage the time allocated was limited hence researcher could not find the information as expected.

CHAPTER TWO

LEGAL FRAMEWORK GOVERNING CYBER CRIME IN TANZANIA

This Chapter examines the role of national, international and regional legislation and frameworks in the prevention and combating of cybercrime. It finds that legislation is required in all areas, including criminalization, procedural powers, jurisdiction, and international cooperation. The Chapter highlights a growing legal fragmentation at international and national level**.**

Cyber space is the space between two networks. Joseph Migga Kizza[23] defines Cyber Space as the concept of an environment made up of invisible information. When computer users log onto the internet, they are able to perform various tasks and Services like browsing the World Wide Web, chatting with fellow cyber citizens, transferring files from one computer to another, remote logging to another computer, sending electronic mail, conducting electronic commerce, video conferencing and more**.** The numerous functionalities and freedom of use while in the cyber space brings an equal ease of committing both immoral and illegal acts[24]

The legal framework creates a controlled environment against virtual crimes that threaten national security and stability. Also, it provides legal guidelines to bring, to identify and charge crimes committed through or in electronic transactions and e-commerce that threaten business growth between companies, organizations, consumers, suppliers and other service providers[25]. The hereunder are the international Legal Instruments that have attempted to shed light into the eyes of enforcement agencies in prosecuting Cyber criminals.

Meaning of cyber bulling;

---

[23] Kizza M.,(2003)., Ethical and Social Issues in the Information Age, (2nd edn), Springer.
[24] Frolence Tushabe, and Venansius Baryamureeba, (2007)Cyber Crime in Uganda: Myth or Reality?, International Journal on Social, Behavioral, Educational, Economic, Business and Industrial Engineering., Vol:1(8) at P.1.
[25] David K., Cyber Crime Laws in the works, The guardian newspaper of 15th April 2013, IPP Media Group, Dar es salaam.

2.1 International Legal Instruments on Cyber Crimes

2.1.1 Extradition Act41

It was always a practice that criminals who committed crimes against the United Republic could ran to hide in other jurisdiction. Police Force Cyber Crimes Unit (PFCCU is vested with investigative, search and seizure and arrest powers[26]. Police is responsible for interviewing suspects, and victims. The information collected is usually piled up and present the case in court save for acts constituting serious crimes where the police cooperates with the prosecutor who assumes chief responsibility for conducting prosecutions[27]. Generally, PCCU have powers to enforce the cyber crimes Act with its subsidiary legislations

2.1.2. International Telecommunication Union

The International Telecommunication Union (ITU), is a specialized agency within the United Nations, plays an imperative role in the standardization and development of telecommunications as well as cyber security issues. Among other activities, the ITU was the lead agency of the World Summit on the Information Society (WSIS) that took place in two phases in Geneva, Switzerland (2003) and in Tunis, Tunisia (2005). Governments, policymakers and experts from around the world shared ideas and experiences about how best to address the emerging issues associated with of the development of a global information society, including the development compatible standards and laws[28]

Until now there is no any universal cyber crime convention.

---

[26] Part II of the criminal procedure Act, Cap 20 R.E 2002 read together with Section 31 of the Cyber Crimes Act, 2015

[27] O‟conner, V.,(2012) Common Law and Civil Law traditions. International network to promote rule of law.

[28] http://www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the Meeting Report of the Third Facilitation Meeting for

2.1.3. Budapest Convention on Cyber Crimes, 2001.

The Budapest convention with its respective protocols though in place is largely a product of regional collaboration, reflecting conditions and premises among Council of Europe member states. As of August 2015 only 47 member states had ratified the convention[29].

The convention aims principally at harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber crime.

Also, the convention aims at setting up a fast and effective regime of International Corporation.

Kizekova[30] asserts that, Russia has been against the convention stating that the convention violates the Russia constitution by permitting foreign Law enforcement agencies to conduct investigations within Russia boarders via the internet.

In 2011, China, Russia, Tajikastan and Uzbekistan tabled a draft of the international code of conduct for enforcement security before the (UN General Assembly 2011). The code seeks observance of human rights and freedoms within the information space[31]. Respect for the sovereignty, territorial integrity and political independence of all nations is also addressed and the code pushes for the development of transparent multilateral and democratic international internet governance arrangements

2.2. Domestic Legal and Institutional Framework

In a move to fight cyber crime and protect citizenry from falling prey to cyber criminals, the government of Tanzania enacted a number of Laws whose aim was to ensure protection of

[29] Cameron B., investigating and prosecuting cyber crimes: Forensic dependencies and barriers to justice, International Journal of Cyber Criminology 9(1) jan-june 2015

[30] Kizekova A.,(2012) The Shanghai Cooperation Organisation: challenges in Cyber space-Analysis. RSIS commentaries, No. 033/2012

[31] Brown, D., (2015) Cyber Attacks, Retaliation and Risk: Legal and technical implications for Nation-States and private entities. In J.L Richet (ED) PP166-203

electronic transactions and personal data information as well as ensure security on the cyber space.

Before 2015, Tanzania had no specific laws to regulate cyber space. However, there were in place some pieces of legislations which catered for some cyber crimes. These include

2.2.1. Cyber Crimes Act, 2015 and the Electronic Transactions Act, 2015

The overwhelming challenges arising out of growing number of internet users, computer system and increased number of false statements in social media compelled the government to enact the Cyber Crimes Act,[32] with the purpose of controlling internet usage, social media and specifically to criminalize offences related to usage of computer system and information technology[33]. Cyber crimes Act 2015 enhances security in cyber space by criminalizing certain activities which pose a threat to electronic transactions. Examples of such activities include; computer related forgery, illegal data interference, and illegal system interference just to mention but a few. But however good it may sound, this Act has incurable defects. For example, though it does have extra territorial jurisdiction, it is very difficult to enforce it and exercise it. While the admissibility of evidence in those cases is governed by the electronic transactions Act which provides for a legal framework for executing electronic transactions, e-governance transactions, and admissibility of electronic evidence.

[32] N0.14 of 2015.
[33] Alex I.,(2015),Defamation in social media, Legal perspective in Tanzania. Reachable at bshabakaki@gmail.com

2.2.2. The electronic and Postal Communications Act (EPOCA)

EPOCA came into force in 2010. It repealed and replaced two pieces of legislations in the Tanzania communications sector. (The broadcasting services Act and The Tanzania communications Act). EPOCA was enacted with three main objectives. These include firstly, *addressing the challenges posed by modern technologies, to harmonize and consolidate communication laws in order to overcome regular conflicts in their implementation, and lastly to introduce the central equipment identification register and registration of SIM cards*[34]. Among others, the Act regulates electronic communication including internet communication and social media; however the Act provides that issues of content will be governed by the Minister of Information, Youth, Culture and sports. The mischief for which the Act was intended to cure appears to be inter alia, computer frauds through mobile phones so the Act could not cater for all cyber crimes thereby necessitating the enactment of specific legislation for that purposes as follows below

2.2.3. The Penal Code44

This is the foremost law of crimes in Tanzania. This is a legislation which was enacted to deal with conventional offences and punishment to those offences[35]. It is the basis for main principles of criminal litigation in Tanzania. Before the advent of new cyber crimes legislations of 2015, the penal code could cater for cyber offences. Both Acts are still depending on each other as they serve as „functional equivalences". The cyber crimes Act, 2015 is a penal code for online offences which ought in some circumstances to borrow principles from the penal code especially where there is a lacuna.

[34] A, Makulilo., (2011) Registration of SIM cards in Tanzania: a critical evaluation of the electronic and postal communications Act, 2010. Computer and Telecommunications Law Review
[35] the penal code Cap 16 R.E 2002

The Act confers jurisdiction to the courts to try any person who commits an offence against the United Republic whether that person is in or outside the territories of Tanzania[36]. The basis for jurisdiction may also be established when a person commits an offence in an aircraft registered in Tanzania[37].

2.2.4. The police force Act

I n Tanzania issue of investigation is usually carried out by police department virtue to section 5 of the police force ordinance[38] here referred to as PFO the power of the police describe as preservation of peace, maintenance of law and order the prevention and detention of crime, the apprehension, protection of the property, the other power such as summon; arrest warrant. Police officer are divided in to four categories Ordinary police officer, Trained people military ,Untrained military .However other person may carry investigation in particular public officer with specific law such tax law investigation of Bureau of the custom department and Anti corruption Bureau the police are very much advantage because they necessary facilities on top wider power. The Police Force and Auxiliary Services Act[39] governs the operation of the Tanzanian Police Force.

The Act must be read with the Police Force Service Regulations of 1995 and the General Orders .Crime prevention is specified in the 2002 Act as one of the functions of the police force. Moreover, the General Orders make explicit the importance of visible policing.

It stipulates that police patrols should be carried out regularly, that the patrolling officer should sign in at different stations en route, and sets out the required discipline and behavior of the

[36] Section 6 of the Act.
[37] Section 6(c) of the penal code Cap 16 R.E 2002.
[38] Police Force and ordinance Services Act Cap 322 of 2002
[39] Police Force and Auxiliary Services Act Cap 322 of 2002

patrolling officers .The Auxiliary Police force Act[40] No 19 of 1969 legalized the establishment of Auxiliary Police. However, this is not a national body with a nation-wide mandate, but units that are established on an ad hoc basis to maintain order and protect property in a declared area.

It is the President who grants permission for the establishment of an Auxiliary Police Unit in a particular and declared area. The rationale for the establishment of Auxiliary Police Units appears to be that they take pressure off the Tanzanian Police Force, cost less to recruit and maintain, have detailed knowledge of a particular area, and are more representative of and responsive to the community in which they operate .is unclear whether the mandate for each Auxiliary Police Unit is identical, and indeed what this is

2.3. Regional Instruments

Arrangements have been finalized for members of the East African Community (EAC) to promote the exchange of information between criminal justice and law enforcement counterparts among Member States of the East African Community on issues pertaining to the fight against cybercrime.

Under the arrangement; Uganda Kenya and South Sudan as well as Ethiopia and Somalia formed the Eastern African Cybercrime Criminal Justice Network to create a network of focal points for law enforcement agencies, prosecution services, and central authorities in order to facilitate informal and formal modes of cooperation in criminal matters involving cybercrime and electronic evidence, In East Africa, cybercrimes take advantage of weaknesses in cybercrime law and the hopeful systems of law implementation leading to a creation of illegal activities. Like the

[40] ibid

rest of the African countries, these criminal activities have troubled the East African region (Burundi, Kenya, Rwanda, Tanzania and Uganda) and demanding the progress of local regional shared networks intended to assist taking the initiative crime prevention and the declaration of operational cybercrime law.[41] Presently, Tanzania is in the process of enacting three laws in line with Cybercrimes. The draft Bills are: the Computer Crimes and Cyber Crimes Bill, the Data Protection and Privacy Bill and the Electronic Transactions and Communications Bill. This because of the increasing number user of electronic communication like Internet, online Bank System network. Some of challenges that Tanzania face in this period of lacking cybercrimes is no specific laws on cybercrime which complicates the process to prevent that action, Insufficient capacity in electronic investigation and the police have not skills to conduct electronic investigations, Lack of awareness among the general public about cybercrime. This cause the some cases of computer criminal to be reported in Tanzania[42].

The government of Kenya established a committee in June 2013 to driving force efforts against cybercrime under the Communication Act of Kenya. By this Act, war was declared on cyber criminals with stiff penalties prescribed for unlawful acts like cyber hacking, and cyber bullying. The Act aims to protect the government within the overall system of ICT as the engine for e-commerce and e- governance to safeguard development. Technically, Kenya Information and Communications Act host the electronics and transactions law. This legislation also provides for cybercrime in Kenya and has provisions on mobile money transactions. The Act also complies the AU Draft Convention on Cybercrime[43]

[41] www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
[42] idem
[43] idem

Rwanda in Cyber law is included in Rwanda's Organic law. Under the Penal Code, section 5 refers to computer related crimes. The penalties include the payment of fines of between 5 to 7 mill. RF. Recidivists are also punished with the same penalties. There are no specific legislations to deal with cybercrimes, but these will be developed in due course. Rwanda hopes due to collaboration at the local, regional and international levels on how to streamline legislation on cybercrime in Rwanda. Rwanda expects that the workshop will help participants analyze current and draft legislation of participating countries in terms of their consistency with the Budapest convention on cybercrime; the rule of law; and elements of cybercrime enforcement strategies[44]

In Uganda, Cyber security is a relatively new field as its study is directly related to the rise of digital technologies. This also means that cyber security has evolved apart from most other concepts of security. This notion of security includes protection from disruptions in confidentiality, integrity, availability and often non repudiation of digital technologies and information. Uganda has recently passed three laws related to the EAC Legal Framework: the Computer Misuse Act, 2011, the Electronic Transactions Act, 2011 and the Electronic Signatures Act, 2011.

The Computer Misuse Act is the principal legislation covering cybercrime. It provides for the safety and security of electronic transactions and information systems, the prevention of unlawful access, abuse or misuse of information systems including computers and for securing the conduct of electronic transactions in a trustworthy environment. The act creates offences with respect to the unauthorized use, access, abuse of computers or data. It also has provisions on electronic fraud, child pornography, and cyber harassment, cyber-stalking. The Electronic section 45 Transactions Act provides for the use, security, facilitation and regulation of

[44] idem

electronic communications and transactions as a functional equivalent to the already existing forms of communication. The Act gives legal certainty in respect of validity, legal effect and enforceability of information in electronic form with respect to relations between parties especially establishing contractual obligations[45]

Burundi in Burundi Cybercrime is relatively new although there is no specific legislation to criminalize unlawful cybercrimes; the Penal Code 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 development of information technology has had consequences which are exemplified in a new kind of crime in cybercrime. Previously, the Criminal Code of 1981 did not punish intrusive behaviors in computer systems and data such as cases of forgery and use of forged material through computer including the modification or destruction of stored data, treated or transmitted by a computer system, and the unauthorized access to a computer system (hacking). Presently, there is a draft bill on electronic signatures and its authentication, consumer protection, privacy, data protection, computer crime, banking and taxation and information security element[46]

2.4. Institutional Framework of Cyber Crimes in Tanzania

There are various institutions which are vested with powers to investigate and prostitute cyber crimes in Tanzania. These institutions include; „*Cyber division in the office of pubic prosecutions'*. Its roles is to coordinate investigation and prosecute cyber crimes, to review and propose policies, laws, regulations, guidelines and standards on the management of fraud, corruption and cyber crime**.**

[45]M. Gercke, Understanding Cybercrime:Phenomena, Challenges and L egal R esponse, ITU Publications retrived Kampala university, Uganda 2012, 45.
[46] Alex I.,(2015),Defamation in social media, Legal perspective in Tanzania. Reachable at bshabakaki@gmail.com .

2.4.1. The Tanzania Communications Regulatory Authority (TCRA)[47]

TCRA is a quasi-independent government body responsible for regulating the communications and broadcasting sectors in Tanzania. The function of this institution is *inter alia*; to issue license and regulate electronic communication systems.[48] TCRA plays the role of regulating telecommunication companies, by tracing for instance electronic transactions and communications which are associated with the commission of crimes.

2.4.3. National Computer Emergency Response Team (CERT)

The main functions of this organ is to coordinate, respond to cyber security incidents at the national level and cooperate with regional and international entities involved in the management of cyber security incidents[49]

[47] Cyber crime response, investigation and prosecution. Encyclopedia of information assurance. New york: Taylor and Francis
[48] Schwartz,K.E., (2009) Criminal liability for internet culprits: the need for updated state laws covering the full spectrum of cyber customization
[49] idem

CHAPTER: THREE

CRITICAL ANALYSIS ON CYBER CRIME PROTECTION AND PREVENTION BY TANZANIA POLICE FORCE

Cyber prevention it's an act of restricting, suppressing, destructing, destroying, controlling, removing or preventing the occurrence of cyber attacks, in either computer system or other devices both hardware and software system, network and data, or any other electronic devices capable of being computer (capable of performing logical arithmetic and memory functions) from such attacks[50].

The government through the agencies especial the Police Force Cyber Crime Unit and other Institution by use of Cyber Crime Act and other Regulation relevance to crime of such in nature can be use in Tanzania to deal with Cyber Crime offences[51]. Generally, CID deals with investigations of crimes, of which cyber crimes are among the crimes investigated by the department.

It also deals with the following function namely: the prevention of crime, investigation and detection of serious crimes, collection and collation of all information regarding crime in the country so that the Inspector General and the Government may be kept informed in all matters of criminal interest, the maintenance of close and effective liaison with all branches of the Force and, in particular with the General Duties Branch, the maintenance of criminal records and statistics and the provision of advice and assistance in all investigations giving rise to the difficulty or doubt and the seeking of legal advice as may be necessary.[52]

---

[50] s41 of the electronic transactions Act 2015.
[51] idem
[52] Section 3(a) of The Police General Order No. 8 of 1961,2nd edition, (2006)

The regulation tries to protect the general public from cyber crime offence, this is done as follows.

3.2 Cyber-crime Investigation Agencies in general

In Tanzania it is the sole of the police force to conduct criminal investigation in general, there are number of police departments. In respect of matter of cyber-crime then Police Force department of cyber Unit is responsible for investigating of offences of such nature. The laws of the land do require that the case should be handled with no delay for the proper adherence of the principle of dispensation of justice. Un dully delay of dispensation of justice amount to the violation of the right to human right. What amount to delay of police investigation the case? In case of ***R V Abdurahmi Msagati***[53]. The accused was charged of Murder, the incident happened 2005 but until the 22nd may 2014 the case was still in the preliminary inquiry stages (under police investigation). Then for such instance it amount to delay of investigation of the case.

3.3 Detailed Reason for the delay of Hearing Cases of Cybercrime.

The right to due process is a broad term, but in this reason the focus will be on the right to be treated fairly, efficiently and effectively by the administration of justices. The right to due process place limitation on laws and legal proceedings in order to guarantee fundamental fairness and justices. Due process is interpreted here as the rule administered through court of impartiality, the issue is whether the present system of administrative set up facilitate the administration of justices.

[53] Cr. Case No. 22 of 2005, Resident Magistrate Court of Kivukoni at Kinndon.

3.4 Relationship between Investigation Machinery and the Prosecution.

The investigation and prosecution are agencies depending to each other for the purpose of administering of justices in case proceeding. Each one depend one another to discharge its duties on the prosecution cases. The investigators to cybercrime are the Police Force cyber Unit who are responsible for collecting the material facts fact for the purpose of evidence then after whole process then they ought to handle to the prosecution to proceed with the case[54].

3.5 Protection against illegal Access

It is not rebuttable that it is from this development of science and technology which mostly affected the developing countries.

The legislation provided that, a person shall not intentionally and unlawfully access or cause a computer system to be accessed. Sub section (2) of section provide that "a person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine of not less than three million or three times the value of the undue advantage received, whichever is greater or to imprisonment for a term of not less than one year or both.

Thus the prohibiting illegal access, person's property and information have prevented the unlawfully access to the other person phone, or computer. Data, network and system can be secured.

[54] Said, M., The Status of Cyber Crimes in Tanzania. A Presentation at the Octopus Conference on Cooperation Against Cyber Crimes & 10th Anniversary of the Budapest Convention, Strasbourg, France.

3.6 Protecting against illegal Remaining

The Act provide that, a person shall not intentionally an unlawfully remain in a computer system or continue to use a computer system after the expiration of time which he was allowed to access the computer system. A person who contravenes subsection (1) commits an offence and is liable, on conviction to a fine of not less than one million shillings or to imprisonment for a term of not less than one year or to both[55].

Preventing illegal remain would protect (prevent) someone's property and information from being infringed online. If they are protected then it means they are secured. This provision is dealing with system security in cyber security.

3.7 Protection against illegal Data interference

A person who intentionally and unlawfully damage or deteriorates computer data; deletes computer data; alters computer data; renders computer data meaningless, useless or ineffective; obstructs, interrupts or interferes with the lawful use of computer data; obstruct, interrupts or interferes with any person in the lawful use of the computer data; access to computer data to any person authorized to access it, commits an offence and is liable on conviction, to a fine of not less than ten million shillings or three times the value of undue advantage received, whichever is greater or to imprisonment for the term not less than three years or to both[56].

The transmitting the other person unlawfully is also is incriminated and it's punishable for the term of one year in prison or a fine not less than two millions shillings or saving both fine and imprisonment.

[55] Section 5 of the cybercrime Act, No. 13 of 2015.
[56] Ibid S 7

These cyber securities provide for prevention to person who wants to unlawfully access data or computer or mobile phone system of another person.

3.8 Protection against Disclosure of details of investigation

A person shall not disclose details of a criminal investigation, which require confidentiality. Then if a person contravenes subsection (1) then the person committed an offence and is liable on conviction to a fine not less than ten millions shillings or to imprisonment for a term of not less than three years or to both[57].

This provides security to data investigation institutions as data are prevented from being disclosed unreasonably.

3.9 Protection against illegal system interference

A person who interferes an unlawful hinders or interferes with (a) the functioning of a computer system; or (b) the usage or operation of computer system, commits an offence and is liable on conviction, to a fine of not less than two million shillings or three times of value the undue advantage received, whichever is greater, or to imprisonment for a term not less than one year or to both[58]

[57] Ibid S8
[58] Ibid S21

3.10 Protection against illegal device

A person shall not unlawfully deal with or possession (a) a device including a computer program, mobile software, that is designed or adopted for the purpose of committing an offence (b) a computer password access code or similar data by which the whole or any party of a computer system is capable of being accessed with the intent that it be used by any person for the purpose of committing an offence.

Occasionally a person may use unlawful program to remove or gain access to certain computer program. For example crack blocking program.

3.11 Search and seizure

The Act allow Police Officers to enter into any premises[59] where a crime has been suspected to occur and search any relevant evidence purporting the occurrence of the said crime, and seize it for the further proceedings. The Police Officer may also extend the search or similar accessing to another system where a law enforcement officer conduct search has ground to believe that the data sought is stored in another computer system or part of it[60]. Search and seizer my prevent any cybercrime from happening as the fact that if the Police officer find something illegal which was about to be used in committing a crime may be prevented.

3.12 Use of forensic tools and the challenge to the insufficiency tools

Cyber Forensic is the process of recovering evidence from digital Medias. According to Robbins definition, computer forensics involves the preservation, Identification, Extraction and documentation of computer evidence stored in magnetically encoded data.[61]

---

[59] idem
[60] idem
[61] www-all-about-forensic-science.com/cyber-forensic htlml, accessed on 15/1/2019

Cyber forensic expert has been defined has a person specialized in practice of investigating computers media for the purpose of discovering and analyzing available deleted or hidden information that may serve as a useful evidence in legal matters.[62]

According to respondents information, they revealed that, the department lacks the common cyber forensic equipment such as red hawk which is a tool used to analyze the suspect computer data, the Evidence Prime which is an advance forensic tool for evidence acquisition from computers using Microsoft windows operating system and another important tool mentioned is the Secure Hash which is an equipment which is used to build a file list with other Vital Information such as file size, Location ,and date of creation [63]

This has made many cases to take longer in investigation due to failure o the department to have these tools for the purpose of effective investigation of cyber crimes in Iringa municipality. The following table below present number of cases reported from 2016-2018

CASES UNDER INVESTIGATION[64]

Figure: 01 showing the cases under cybercrime in stage of investigation.

Year	Identity theft	Cyber defamation	Cyber stalking	Fraud
2016	2	0	0	4
2017	13	1	1	2
2018	16	2	1	5
Total	**31**	**2**	**2**	**11**

Source; Iringa Resident Magistrate Court

[62] www.exepertlaw.com/liabrary/forensic-evidenece/computer-forensics-101.html , accessed on 15/1/2019
[63] Police Registry,Iringa municipal
[64] Iringa Resident Magistrate Court Report 2018.

The above table shows number of cases which are under investigation by the cyber crimes unit under the office of DPP in Iringa region. The results shows that 54 cases are under investigation out of 68 cases reported in 2016-2018

The results from the above table shows that many cases are still under investigation. The respondents were asked as to why many cases take long time to be investigated. The researcher observed that many cases take long time to be investigated, because the Criminal investigation department at Iringa lacks enough cyber forensic equipment's.

MENTION

Figure: 02 showing the cases in mention stage

Year	Identity theft	Cyber defamation	Cyber stalking	Fraud
2016	0	0	0	0
2017	1	0	0	0
2018	2	0	0	0
Total	**3**	**0**	**0**	**0**

Source; Iringa Resident Magistrate Court

The above table present number of cybercrimes that has been mention from 2016-2018. The results shows that only 3 cases have been mention out of 68 cases which have been reported within the three years. The researcher observed that the major problem is due to lack of cyber forensic expert and equipment on investigation of cyber crimes. As the results few cases appear to be taken to court.

HEARING

Figure: 03 chat showing cases under the hearing stage

Year	Identity theft	Cyber Defamation	cyber stalking	Fraud
2016	0	0	0	1
2017	0	0	0	0
2018	0	0	0	2
Total	**0**	**0**	**0**	**3**

Source; Iringa Resident Magistrate Court

The above table present cases on hearing from the reported cases since 2016-2018, in which the results shows that only two cases are upon hearing and yet until now the cases are still in court due to lack of sufficient evidence. The researcher observed that such problem has been caused by lack of cyber forensic expert and equipment's which does not allow effective investigations by the CID.[65]

Where a law enforcement Officer is satisfied that essential evidence cannot be collected then he may apply to the court for the order of authorize the use of a forensic tool(s). Such any an application must describe the name of suspect, address, targeted computer system, and a description of the intended measures, purpose, extent and duration of the utilization. The law enforcement Officer shall ensure that any modification made to the computer system or computer data of the suspect are limited to the investigation and that changes reversed after the completion of the investigation is restores into the system[66].

There are difficulties which might be encountered during the investigation such as difficulties of find the actual evidence to support their claim on the said crime committed or about to be

[65] idem
[66] Ibid S 31

committed. It is at this moment whereby an expert or experts relating to forensic knowledge must be employed so as to detect the actual evidence in support of the said crime or the crime to be committed. This specialist may deploy or install a number of electronic device or methodologies or forensic tools[67] so as to help them detecting the information or data or anything relating to the commission or attempt to commission of the investigation permit the possibility of preventing a cybercrime through detecting either information or installed device which were planned to be used in electronic devices for commit a certain crime, whether is for hacking, cracking and other related crimes, and controlling it from further commission.

3.14 Manner of dealing with cyber-crime Offence in Court

The law require that all cases to be tried or being institute to the court with proper and competent jurisdiction.

The manner of instituting cyber-crime offences is normally by way of charge where it contains the particulars of the suspect, the particulars of the offence and other relevant information.

Where the Police investigation is ready then the prosecution tables the case to the court of law for the further proceeding such as preliminary hearing of the case, examination of witness and evidence tendered by both parties to the court of law.

The mechanism of dealing with cyber- crime especially this relating with the theft through Mobile Phone network is much centralized and thus what brought a contradiction to the researcher to go and find the thesis of the research on such particular problem especially to the designated area of study which is Iringa.

[67] Ibid S 37

3.14.1 General data and information to be obtained to the main companies

The information or particular which are relevant to the case such as records of transaction are only available to the main company through the general manager. Such request of those data from General Company normally takes time thus cause the un-reasonably delay of the administering justices by court. And this contravenes The constitution of United Republic of Tanzania of 1977 and other laws of the land provide for the right of fair and speed trial of the case, and this is one of the important pillars in relation to rule of law. That justice should be done to all equally and court should resolve matters before them within the reasonable time and with unduly delay.

Article 107A(2) provide as follow in delivering decision in matters of civil and criminal in nature in accordance with the laws, the court shall observe the following principles, that is to say[68] Impartiality to all without due regard to one's social or economic status ,Not to delay dispensation of justice without reasonable ground. As it has been shown in case of Republic V Abdul Nondo the case was before the Resident Magistrate Court at Iringa region has closed up the testimony of the Counseling Faculty of the Student Network Abdul Nondo after hearing two defense witnesses, where he scheduled October 2 to specify the day of judgment of the case.

Before closing the evidence, Judge Iringa Regional Court Judge Liad Chamshama has heard two witnesses on the side the defense witness where the first witness is Abdul Nondo and the second witness is Alphonce Lusako. Giving a witness before the Judge yesterday Abdul Nondo led by his lawyer Jebra Kambole, Nondo claimed to have been captured by unknown people near the College's College Water Ubungo at five o'clock in the night, on March 6, 2018, with the throw and throwing the backbone into the car. While the prosecution said intended to bring their

[68] The Constitution of United Republic of Tanzania of 1977.

witness who was the general Manager of Tigo Mobile phone network Tanzania Dare salaam headquarter who was not able to appear on time due to the other official responsibility outside the country.

Nondo said the people were The question is why they are used by politicians to disrupt peace and accused him of being chaired by Chairman Chadema Freeman Mbowe, Zitto Kabwe and Hellen Kijo Bisimba (former Director of Human Rights and LHRC) as well as accusing him of being Kimange's agent in the preparation of student protests but has denied such suspicions.

For his part, second witness Alphoce Lusako, who is a direct leader in the TSNP organization, told the court that after receiving information from Paul Kinabo having received a message via telephone from Nondo being at risk and then reporting to college leadership and college assistants and given RB. Prosecutor Abdul Nondo was sentenced to court on March 21, 2018 and read his allegations which he refused to do so on October 2 This year the Court will return to refer to the Day of Judgment.

The system of requesting data, information to Headquarters seems to be improper and just mere waste of time since there are Zone Office in each Region where the information could also be given out and not only relaying to Headquarters

3.14.2. What Is Meant By The Term Delay?

Delay is defined according to subject matter. Mchome S.E. defines delay as case processing time[69]. He adds that the shorter the time of investigation the question of delay does not arise, but the longer the time of investigation the question of delay arises. If one uses the term case processing time for the time needed to process a file through the criminal justice system, this

[69] Sifuni Ernest Mchome in his paper about overcrowding in prison delays of investigation in the administration of Criminal justice, at Ngurdoto Mountain Lodge Arusha 09th May, 2005.

time might be shorter or longer depending on different factors influencing the means of processing: either manual or automated and the means by which the case is cleared. In this category most often we refer to investigators because of the terminology that has, now become a common appendage of our criminal justice *"upelelezi haujakamilika",* meaning investigation is not complete, given for the most trivial cases as some would think. According to **Twaib ,F** [70] in this book the authors have stated inter that showing delays of cases is one of the main subject of complain by the public other seem to believing that that the lawyer and court the court and the official are more to be blame for the delay of the cases that the advocate by the adjournment of the cases by as well the Magistrate example in the case of Weston panja And Mwaisengele V Rose Shirima Mzava As Then Was Had Strike Out The case because it had been mention 36 time the case has take 5 year the other goes father and state delays of the cases is due to bureaucracy lead to inefficiency and consequent injustice example in the case of Ndekerio Ole Matsya V Tanzania Breweries Ltd an appeal took three years to reach the registry of the court of appeal generally the other basing only to the lawyer or advocate, magistrate and bureaucracy system. Howe ever the other fall to showing the factor which lead on delay of investigation in criminal cases

3.14.3. Financial Intelligence Unit[71]

This institution works hand in hand with the police cyber crimes unit to deal with offences such as engagement of person[s] directly or indirectly in conversion, transfer, acquisition of money or

[70] The legal profession in Tanzania the law and practice by dr fauz twaib of 2008 publishAfrica (k) ltd

[71] Established under Electronic and Postal Communications Act, 2010.

property known to be of illicit origin and in which such engagement intends to avoid the legal consequence of such action[72].

3.14.4. Police Force Cyber Crimes Unit (PFCCU).

This institution is vested with investigative, search and seizure and arrest powers.67 Police is responsible for interviewing suspects, and victims. The information collected is usually piled up and present the case in court save for acts constituting serious crimes where the police cooperates with the prosecutor who assumes chief responsibility for conducting prosecutions[73]. Generally, PCCU have powers to enforce the cyber crimes Act with its subsidiary legislations.

3.14.5. E-payments and E-commerce Fraud

Tanzania is on the move to battle the encroaching fraud in the electronic payment system creeping into businesses and resulting in financial loss[74]. Advancement in the tactics used by cyber criminals keep increasing and varying. A local bank in Tanzania was attacked by a wave of card skimming techniques and only discovered the loss of billions of shillings after customers complained that their accounts had been drained. The large amounts of money that these systems process coupled with their insecure configurations has contributed to them being a favorable target for attackers. Even though the government has enacted the National Payment System Bill, 2015, it is critical that these laws and policies be implemented in order to reap the full benefits

[72] Section 124(1) of the Act.
[73] Part II of the criminal procedure Act, Cap 20 R.E 2002 read together with Section 31 of the Cyber Crimes Act, 2015.
[74] Idem

CHAPTER: FOUR

CONCLUSION AND RECOMMENDATIONS

4.1. Conclusion

The aim of this research was to examine how the existing Institution and laws are sufficient to fighting cyber crimes in Tanzania. It undertook to review the role of law in combating electronic crimes in Tanzania to ensure that online consumers are legally protected. The work has also assessed the efficacy of the legal framework in combating cybercrimes in Tanzania. The research has dissected cyber crimes in the country and figured out how it should be eliminated just by use of legal framework or other measures on top can be improvised to ensure that cyber crimes issues are addressed in broader context.

It was observed that society as on today is happening more and more dependent upon technology and crime based on electronic offences are bound to increase. Endeavor of law making machinery of the nation should be in accordance with mile compared to the fraudsters, to keep the crimes lowest. Hence, it should be the persistent efforts of rulers and law makers to ensure that governing laws of technology contains every aspect and issues of cyber crime and further grow in continuous and healthy manner to keep constant vigil and check over the related crimes.

As observed in this Study, information technology has spread throughout the world. Now days, computers are used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development[75]. As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the cyber crimes and as pointed out earlier, the financial sector is the main target. It is for this reason that there is need to

[75] http://www.thecitizen.co.tz/News/national/Banks-under-siege-from-ATM-hackers-/1840392-2631726-u277o6/index.html

adopt a strict law to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber crime[76]. These bodies lack the skills and technology needed to identify cyber crimes and perform forensic investigations that will lead to successful prosecutions of cybercrimes.

4.2. Recommendations

4.2.1 Legal Recommendations

Based on the conclusion above, the following recommendations may be advanced:

The Penal Code and Cyber Crime Act should be amended to provide for criminal activities conducted using computers and computer networks.

There should be decentralization of the system of the Mobile phones Companies to provide data, the regional zone Office should also be providing required data and information for the prosecution.

The offences that should be introduced in the Penal Code are hacking; illegal access to computers and computer networks, fraud committed using computers and computer networks, money laundering and related crimes, identity theft, sniping and many others[77].

International cooperation is also vital in cybercrimes. It is recommended that there should be a convention at the international level similar to the one which is operational in the European Union[78].

There should as well be training for judges, magistrates, investigators and prosecutors on cyber crimes

[76] https://faculty.haas.berkeley.edu/przemekj/Mobile_Money.pdf
[77] Developments in global law enforcement of cyber crimes policing. International Journal of police strategies and management, 29(3) 408-433
[78] *idem*

Harmonization of International Conventions; It is further recommended that for cyberspace to be properly harmonized there should be corresponding of International Conventions to the domestic legal framework; that when the municipal law concurs with International Conventions becomes easier for the national law in adopting the rapid changed of e-technology and thus allow for timely easy adjustments to the domestic laws in case of new inventions and similar changes[79]. As Traders and individuals are becoming more and more reliant on information technology to smooth the progress of international business transactions and many spectators believe that full-fledged electronic commerce is nearing a reality. Concurring with International Conventions will offers advantages such as security, lower costs and quick and efficient access. For instance in the business community uses a system known as electronic data interchange (EDI), because EDI offers advantages such as security (closed network), lower costs and quick and efficient access, it is thought that any international industry would benefit greatly from its adoption. We will also extend the level of technology integration in the market on the global spread of e-commerce and report on the primary aspects from an international perspective[80].

4.1.2 Extra Legal Recommendations

Educating the Community to Protect Themselves

As with crime in the physical world, no amount of action by government and the private sector can prevent every cybercrime, those of us who use digital technologies have to take responsibility for our own security and safety and exercise safe practices[81]. Most instances of financially-motivated cybercrime like social engineering fraud and ATM skimming, identity theft can be prevented by taking simple steps or by knowing what to look out for. Governments

[79] http://www.ihrr.net/files/200655%20/state-sovereignity-int-legality-morality-roth-2005-pdf
[80] Article 2(4) of the United Nations Charter, 1945
[81] http://www.reporterhelard.com/news/loveland-local-news/ci_23174314/lovelands-cyber-crimes-unit-grows-but-still-sees

and private sectors can assist users to understand these steps and to recognize the warning signs, this can be achieved by conducting awareness programmers through different media.

Fostering an Intelligence Led Approach

Criminals are quick to find ways to exploit new technologies to further their illicit activities. Authorities like Police Force, TCRA, BOT and SSRA must stay up-to- date with these methods so that they can recognize emerging trends, patterns and problem areas. Sharing quality, timely and comprehensive information and intelligence will lead to better understanding of cybercrime and more effective responses[82].

Improving capacity and capability to fight cybercrime

The capacity and capabilities of our agencies, particularly law enforcement agencies, need to keep pace with evolving technologies if police are to perform their duties in the digital environment. At the most basic level, all police officers need to know how to gather and analyze digital evidence, leaving specialist units to focus on more complex cybercrimes. Specialist units within law enforcement agencies must have the training and capabilities to detect and investigate the more complex and sophisticated use of technology in criminal activities[83].

Identity Theft

Identity theft is a crime whereby cybercriminals impersonate specific individuals. This is particularly prominentduring sim card registration where fake identity during sim card registration was noted. This year we have witnessed the Tanzania's telecoms regulator fine six

[82] Police officer for investigation, cyber crimes unit.
[83] Kanyabuhinya B., Course Instructor, Economic and Cyber Crimes Law, University of Dar es salaam School of Law.

mobile phone operators Tsh552 million ($258,000) for laxity in sim card registration[84]. The fines came less than three weeks after the Tanzania Telecommunication Regulatory Authority (TCRA) switched off 1,830,726 IMEIs[85].

Collaboration.

There is need for Government, Private Sector and Academic institutions to have forums that discuss and tackle these cyber security challenges. In the Private sector we have and see different challenges and threat actors. Sharing of solutions trends, intelligence and research is vital to keeping abreast in this dynamic field. As shown in the Costech funded – State of website security report -April 2016 of Gilbert Kilimba. It enables us to gauge where we havegaps in IT Security Practices[86].

Assisting prosecutors and the judiciary to deal with cybercrime and digital evidence.

Prosecution of cybercrime offence is an important part of the enforcement framework to deal with cybercrime and assists in creating and maintaining public confidence in our criminal justice system, in order for cybercrime offences to be prosecuted effectively prosecutors and judicial officers need to be able to understand and evaluate technical digital evidence[87]. While courts and the legal profession are becoming more accustomed to the use of new technology to commit crime, the admission of digital evidence can still be a technical process[88]. As the use of technology in crime grows, prosecutors and judges will increasingly be required to present and understand highly technical details in order to effectively administer the cybercrime Act2015 and

[84] HCT-00-CC-CS-857-2007[2010]
[85] idem
[86] http://www.reporterhelard.com/news/loveland-local-news/ci_23174314/lovelands-cyber-crimes-unit-grows-but-still-sees
[87] idem
[88] Supra note 80

the like. Government can continue to assist prosecutors and the judiciary by providing the resources they need to respond to legal concepts associated with the new technology and the facilities they need to analyze and consider digital evidence in a court setting[89].

Cloud – Based Solutions

Many organizations in Tanzania are steadily embracing cloud computing solutions for different business and technological benefits. Majority of these organizations have adopted cloud applications services like Oracle cloud and Microsoft 365[90]. From a security perspective, this trend has given rise to two security issues; traditional security controls can no longer help protect local business critical systems. Also Tanzanian companies are losing visibility of their security posture. It's therefore paramount that even with cloud adoption; businesses should review the Service Level Agreements and contracts with the cloud providers to ensure security of their data[91]

Cyber Security Firms.

Cyber security firms have the advantage of large attack-knowledge base. This puts them in a unique and important position of providing visibility into the cyber threat landscape for the other players in the ecosystem and Organizations need to document information security policies with relevant controls that will guide the implementation and operation of information security[92].

[89] idem
[90] http://www.dailynews.co.tz/index.php/home-news/45592-big-telecoms-five-fined-for-cyber-crime-inaction
[91] http://www.ega.go.tz/uploads/publications/
[92] https://www.tzcert.go.tz/

BOOKS

Brainbridge, D. **"***Introduction to Computer Law***,** Pearson, Education London, 5th Ed (2004).

Carol, J.M, **"***Computer Security***",** Butterworth's and Company, London, (1997).

Cavazos, E & Morin, G., *Cyber Space and the Law: Your Rights and Duties in the On-Line World***,** 4th Edition, the MIT Press, London, (1996).

Mambi, AJ. ICT Law book: A Source Book for Information & Communication Technologies and Cyber Law, Mkuki na Nyota, Dar es salaam 2012.

Tavani, H.T. Ethics and Technology, 2nd Ed, John Wiley & Sons Inc, USA 2010.

Edwards L. & Chalotte W, Law and the Internet, 3rd ed.(united state: Hart Publishers, 2009)

Reyes. A & Kevin. O, Cyber Crime Investigation2nd ed (New York: Hart Publishers 2007

Robert .M, Cyber Crime investigation 2nd E.d (Elsevier Inc, 2011

Daid, L.C, *Computer crimes categories: How Technology Criminals Operate*, Michigan state University, East Lansing Michigan (2010).

Benedict,M.T,(2000) Personal freedom and police power in Tanzania, by C.M, Peter and Juma

I.G. Shivji,(2004) Constitution and legal system of Tanzania

Spack,J, Emmons on criminal procedure (2000)

Sirohi,J.P.S, Criminology and Penology (2006)

Twaib,F "Legal Professional in Tanzania , the law and practice",law Africa publishing(T)LTD, Dar es salaam, Tanzania (2008)

Martin,J and Turner,T.Chris, Criminal law

Ian J. Llyoid, Information technology law 6th ed.(Newyork: Oxford university Press, 2010

African policing civilian oversight forum *Common Standard for Policing* in East Africa, London WCIB 5DS UK. (2010).

Janine S. & Ronnie C, Internet Law and Policy 1st ed.(New Jersey: Pearson Education Inc, 2002

Clean foundation analysis of police and policing in Nigeria, Malthouse press limited, Lagos (2016).

Ekblom P. Crime prevention New York press(2015).

Fereshi E. How investigator ought to deal with violence crimes, Dar es Salam University press Dar es Salaam Tanzania (2013).

Harrendorf S. *et al* International statistics on crime and justice, Oxford university press Limited, London (2016).

Andrew M& Zakayo L, Electronic Transaction and Law of Evidence in Tanzania, (Paramiho: Iringa University College, 2007,
Police headquarter criminal investigation department Report on crime for the period of (2015 - 2017).

Kothari C. R Research Methodology (2014).

JOURNALS

A, Makulilo., (2011) Registration of SIM cards in Tanzania: a critical evaluation of the electronic and postal communications Act, 2010. Computer and Telecommunications Law Review

Brown, D., (2015) Cyber Attacks, Retaliation and Risk: Legal and technical implications for Nation-States and private entities. In J.L Richet (ED)

Cameron B., *investigating and prosecuting cyber crimes*: Forensic dependencies and barriers to justice, International Journal of Cyber Criminology 9(1) jan-june 2015

Frolence Tushabe, and Venansius Baryamureeba, *Cyber Crime in Uganda: Myth or Reality*?, International Journal on Social, Behavioral, Educational, Economic, Business and Industrial Engineering., (2007) Vol:1(8)

INTERNET SOURCES

http://dailynews.co.tz , visited on 18th January, 2019
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en

http://portalsandrais.frbatlanta.org/online-banking-fraud/ visited on 27th February 2019.

http://rbidocs.rbi.org.in/rdocs/Bulletin/DOCs/6270.doc visited on 23th march 2019

http://www.afp.gov.au/national/major_fraud/internet_scams visited on 13th march 2019

http://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en visited on 30th march 2019

http://www.legalindia.in/cyber-crimes-and-the-law

http://www.link.co.uk/Press/NewsReleases/Pages/Fraud_Prevention_Guide.aspx

http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective

http://www.ukpayments.org.uk/payments_industry/payment_fraud/plastic_fraud/types_of_card_fraud