CYBERCRIME AND ANALYSIS OF LAWS: A CASE STUDY OF ZANZIBAR LEGAL ISSUES

ABDALLA HAJI FAKI

DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIRMENTS FOR THE MASTER OF LAW IN INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS (LLM IN IT & T) OF THE OPEN UNIVERSITY OF TANZANIA

2014

CERTIFICATION

The undersigned certify that he has read and hereby recommend for examination a Dissertation entitled, "*Cybercrime And Analysis Of Laws: A Case Study Of Zanzibar Legal Issues*" in partial fulfillment for the Award of Master of Law Degree of the Open University of Tanzania

…….....

Prof. David Mellor

(Supervisor)

Date…….....

COPYRIGHT

DECLARATION

I **Faki, Abdalla Haji,** declare that this dissertation is my own original work, and that it has not been presented and will not be presented to any other University for a similar or any other degree award.

……..

Signature

……

Date

DEDICATION

This work is dedicated to my parents Mr. Haji Faki Mabrouk and Habiba Khamis Salim who took exceptional efforts to send me to school and teaching me on how to live well with others. Special dedication is to my wife Lutfia Abdalla Ali, My children Ahlam, Arkam and Almiras well as my brothers Abdul Wahid and Khamis for their patience, perseverance and understanding throughout the period of intensive study for my course.

ACKNOWLEDGEMENT

The first thanks is to the Almighty Allah who above all deserves an acknowledgment in respect of this work and others for His utmost blessings, protecting, loving and guidance that always leads to my success and giving me strong suit throughout the period of my study at the Open University of Tanzania. Further, I wish to express my appreciative to everyone who has honestly supported my studies. In fact, there is large number of people who in one way or another sacrificed and surrendered their time and energy to encourage me. Although, it is not possible to mention and enumerate all of them, I would like to take this opportunity to thank them all for their useful contribution. However, I may mention a few deserved special gratitude for their greatest efforts in making this work successful. In doing so, I show profound appreciation and good will for being helpful to me.

In the first place, I am heartily thankful to the librarians, officers and technicians at the all institutions which granted permission to allow me to pursue this study successfully. Secondly, I am very grateful to Mr. Omar Sururu, Lawyer from DPP office for his great assistance on searching materials used to complete this work and arranging this work. Surely, he played a very unique role in helping me in the fulfilment of this course.

In addition, I am especially indebted to my supervisor Prof, David Mellor, for his Endeavour to provide prompt and valuable intellectual inspiration and guidance. His constructive criticisms and positive encouragement made this scholarly effort successful. Moreover, I send special gratitude to Course Coordinator Mr. Gervas Yeyeye and the entire academic staff for their time and sharing experience and

knowledge.

I further thank toMr. Issa Mohd Salim and my fellow discussion team of LLM in IT & T studentsMr. Omar Hamim, Mrs. Fatma Masrur, Mrs AmaliaLudovick and Madame Jane for their encouragement and assistance of how the ideas could be arranged so as to bring sense at course and during the preparation of this dissertation. More than that, I would like to extend my special gratitude to my beloved wife and my children. My wife remained tolerant during the whole period of my absence from home and for her moral support she provided to me in inspiring me to work hard. She has always been a key person behind my academic progress.

ABSTRACT

This dissertation is specially based on the researcher study about the cybercrime and analysis of laws: a case study of Zanzibar legal issues. The data collected through interviews, internet and library research with focus on the issue of cybercrime in Zanzibar ; the data was collected from different institutions called Director of Public Prosecution (DPP), High court of Zanzibar, Zanzibar Attorney General Chamber and Ministry of Constitution and Legal Affair, Zanzibar Law review Commission, Police Headquarter and MwembeMadema Police Station, Peoples Bank of Zanzibar, Zanzibar Telecommunication Company ltd, Ministry of Infrastructure and Communication and The State University of Zanzibar. The study will help to fill the gap between laws and cyberspace in Zanzibar and bring benefits to the responsible institutions to initiate legislation specific for cybercrime and amend our laws to meet the requirement in a life of digital technology. Also, the study boarded in studying experiences of international legal response and regional legal frame work in order to identify importance of the innovation and challenges faces the field. And last give the recommendation on issue required to solve the challenge on current legislation.

TABLE OF CONTENTS

LEGISLATIONS

LOCALLEGISLATION

Banking and Financial Institution Act No 5 of 2006

Zanzibar Evidence Decree Cap 5 of 1917

Copyright Act No.14 of 2003

Electronic and Postal Communication Act No 3 of 2010

Prevention of Terrorism Act (URT),2002

Public Services Acts No.2 of 2011

Tanzania Communications Services (Licensing) Regulations 2005

TCRA Act No. 12 of 2003

The Criminal Procedure Act, Act no.7, 2004

The Anti-Money Laundering and Proceeds of Crime Act No. 10,2009

The Children Act 2011.

The Constitution of United Republic of Tanzania, 1977

The Employment Act No. 11,2005

The Zanzibar Anti-Corruption and Economic Crimes Act, 2012

The Zanzibar Constitution 1984

Zanzibar e-Government Policy, June 2012

Zanzibar ICT Policy, First edition, 2013

Zanzibar Law of Contract Decree

Zanzibar Penal Act No.6 of 2004

INTERNATIONAL LEGISLATION

African Union Conventions on cybercrime

EAC Legal framework for Cyber laws EAC 1 and EAC 2

G8 Deauville Declaration: INTERNET

General Assembly resolution 65/230

Resolution 67/184, CCPCJ

The African Centre for Cyber law and Cybercrime Prevention

The Council of Europe Convention on Cybercrime

The East African Community level (EAC)

The UK Computer Misuse Act

The United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI)

CASES

ASP Abrahman V. Ahmed Sultan and Walas Lawrence MAD/RB/ 656 2014

Asha Khamis Ali v unknown MAD/RB/216 15.01.2013.

Trust Bank Ltd V. Le Marsh Enterprises Ltd and others. H.C (Com. Div) at DSM CC No. 4 of 2000 (unreported).

ABBREVIATIONS

AU	African Union
CCPCJ	the Commission on Crime Prevention and Criminal Justice
CEOP	The Child Exploitation and Online Protection Centre
CRC	Convention on the Rights of the Child
DoS	Deniel of Services
DPP	Director of Public of Prosecution
EAC	East Africa Community
EC	Electronic commerce
ECC	European Cybercrime Centre
EPOCA	The Electronic and Postal Communication Act
EU	European Union
FAST	The Federation Against Software Theft
ICT	Information Communication Technology
IP	Intellectual Property
ISP	Internet Services Provider
MDGs	Millennium Development Goals
NCA	National Crime Agency (NCA)
NGOs	Non Government Organization
OECD	Organisation for Economic Cooperation and Development
PBZ	The People’s Bank of Zanzibar
RGoZ	The Revolutionary Government of Zanzibar
TCRA	Tanzania Communication Regulatory Authority
TOC	Convention Against Transnational Organized Crime

UAE	United Arab Emirates
UK	United Kingdom
UN	United Nations
URT	United Republic of Tanzania
USA	United states of America
ZANTEL	Zanzibar Telecom Company Ltd
ZBC	Zanzibar Broadcasting Cooperation
ZSGRP	Zanzibar strategy for growth and Reduction of Poverty

CHAPTER ONE

1.0 INTRODUCTION

.1. Background of Zanzibar

According to the Constitution[1], Tanzania is a state and is a sovereign United Republic and the Territory of the United Republic consists of the whole area of Mainland Tanzania and the whole area of Tanzania Zanzibar and includes the territorial waters[2]. The United Republic of Tanzania (URT) was formed out of the union of two sovereign states, namely, the Republic of Tanganyika and the People's Republic of Zanzibar where in April 24, 1964 Tanganyika (Tanzania Mainland) and Zanzibar signed the union agreement. All state authority in the United Republic is exercised and controlled by two organs vested with executive powers, two organs vested with judiciary powers and two organs vested with legislative and supervisory powers over the conduct of public affairs[3].

The organ vested with the executive powers is the Government of the United Republic and the Revolutionary Government of Zanzibar. The Organ vested with Judiciary powers is the Judiciary of the United Republic and the Judiciary of Tanzania Zanzibar. The organ vested with the legislative and supervisory powers over public affairs is the Parliament of the United Republic of Tanzania and the House of Representatives of Zanzibar.[4] Zanzibar is consist of two main Islands called Unguja and Pemba and other surrounded small Islands. The first

[1]The Constitution ofUnited Republic of Tanzania, 1977
[2]Ibid 2
[3]Ibid 4
[4]https://www.fiu.go.tz/TanzaniaNationalAML-CFTstrategy.pdf, pg 4, (accessed 9th July 2014).

Independencedate was in December 1963 from the British Empire[5]. In January 1964 the Revolution was take place and now considered as Independent Day. The revolution established The People Republic of Zanzibar under the rule of President of Zanzibar.

According to the article 4 (3) of union, Zanzibar is the semi-autonomous state within in the United Republic of Tanzania. The list of a unionmatter [6]attached to the Article of Union are applied for the whole country and those are out of the lists of union matter is under the Zanzibar Government. Every part of union have its own responsibility on legal issue. The executive organs in Zanzibar are composed by President of Zanzibar as a head of the Government, Zanzibar's House of Representatives which have the power of jurisdiction over all non-union matters, Judiciary of Zanzibar, all cases tried in Zanzibar Courts, Court of appeal is a union matter but has no power on Zanzibar constitutional and Islamic Law (Kadhi Courts)[7].

.2. Background of the Study

Today's, there is a high spreading out of Information Technology surrounding most parts of life in Zanzibar. This makes possibilities for businesses running in Zanzibar to compete with other around the East Africa and international. Some Companies in Zanzibar sells and buys through internet. AlsoDifferent sensitive information are sending through internet during the transaction and communication. The

5 http://www.aaregistry.org/historic_events/view/zanzibar-gains-independence-britain, (accessed 23rd July 14).
[6]Article 4 of the URT constitution
[7]Act No 2 of 2002, the Zanzibar Constitution 1984

technological change everywhereto the world and make of computer and internet as a basic device for communication and make the World as a village. Thus, Zanzibar start to change their traditional means of communication to electronic means.

Also, they use computer for storage of data, processing both private and public information. Cyber society goes virtual the World generated by Technology and it is the Engineering of Information Technology and Telecommunication take responsibility to drives the World. The Government take serious steps to combat cybercrime by made amendment of her laws. But the extra effort will needs to establish strong legislation in order to prevent a cybercrime. Another issue is cyber terrorism, terrorist were attracted to perform their activitiesby using of internet and computernetwork system. They use internet in their communication and simplify money Laundering. So electronic transfer system letthe group of terrorist to transfer their information on their target area.

Zanzibar and Tanzania Mainland in generally have been seeing the rapid improvements in innovations and production of software and hardware technologies. The current offences like hackers, stolen sensitive information and using of electronic commerce to facilitate business and communications will require the cyber law because most case is take out from a computer and related technologies. This means that information through electronic way is very sensitive and a part of technology need cyber law to providing and disapproving a realities in dispute.

As sheakhin cyber Law: Provision and Anticipationthe nature said that; Internet is changing and this new medium is being seen as the ultimate medium ever evolved in

human history, every activity in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain, to the time you setup your website, to the time you conduct electronic commerce transactions on the said site, at every point of time, and there are various cyber law issues involved.[8]

.3. Statement of the Research Problem

The study focus on Cybercrime legal issue in Zanzibar. There is somelaws that deals in cyberspace in Zanzibar. But the laws are inadequate to fight well with the cybercrime crisis. In General we can say there is no statute in Zanzibar for governing Cyber laws. These day a need of strict statutory laws to regulate the activities of criminals is rising around the world together with protect the true sense of Technology. The laws will protect the area such as electronic transaction, electronic commerce e- governance and other activities need digital technology. Also the laws will provide penalties and punishment for any cybercrime activities. In Zanzibar some cases are reported to police and not attending to the court due to lack of electronic evidence binding them.The Zanzibar Evidence Decree still is silent on electronic issue. Until now the evidence in court are in physical means.Therefore Police officer have lack enough expert and technology to suspect an electronic criminal.

Increasing of communication network improve the online business such as electronic commerce, electronic banking, Mobile Money and sending information through emails individual and services/products advertisement. So the current legal

[8]Sheakh, T, Cyber *Law: Provision and Anticipation*, 2012, Vol. 53 No.7.

framework dealing with cyber issue seems to be not adequate to regulate cybercrime because the existing laws are practices to traditional crimes and evidence. Therefore, there are legal challenges concerning cybercrime in Zanzibar which arise many problems to the Lawyers, ICT technicians when applying the laws which do not recognize the new technology when any matter arise.

For the early stage to fight with cybercrime amendment on some laws was done. The Zanzibar Panel Act amended by inserting the number of offence related with computer like inserting or deleting a data without permission, destruction of computer or computer system without permission and other amendment on electronic field.

.4. Objectives of the Study

The study was directed under General Objectives and Specific Objectives. The researcher was study legal and regulatory framework to find out the position of Zanzibar in specificto stop cybercrime.

a) The General objectives of this study is to examine to what extent the laws of Zanzibar are effective to combating cybercrime.
b) Specific objectives of the study are:The study should
    i. Identify the inadequacy of law(s) governing cybercrime in Zanzibar.
    ii. Identify what effortsto be taken by Government to improving laws to combat a cybercrime.
    iii. Identified the challenges that faced Zanzibar laws to combat cybercrime.
iv. Suggest the solution based on experiences drawn from various international legal framework that combat the cybercrime.

.5. Hypothesis

The study assume that there is no specific legal framework that exist to combating cybercrime and existing laws are inadequate to prevent cybercrime because have been applied for traditional cases. Also the study assumes that there is no awareness among the citizen on effects of cybercrime.

.6. Scope of the Study

The study was to observe how Zanzibar combating a cybercrime. The researcher was interest to analyse the legal documents that can be used to stop computer crime. And what effort are taken to make Zanzibar and rest part of the world to be free from cybercrime. The study was focus on strategies that have been initiated by Zanzibar to be free from cybercrime and make a digital life to be better place.

.7. Significance of the Study

The study has the significance in observing the weaknesses present in the law governing cybercrime and strategic to initiate cybercrime law in Zanzibar. Also identify the driving force succeed to solve that problem. Therefore it provided Challenges and suggest better recommendations to the government to combat cybercrime.

CHAPTERTWO

LITERATURE REVIEW

.1. Introduction

There is no doubt that the technology of ICT is growing dramatically with cybercrime. This growth brings a lot of changes and revolutions from traditional methods to electronic means. The change includes governments, business and other activities from paper based to digital. Also introduced new methods of banking and other financial transaction under electronic system. The impact of digital technology is going very fast and cause the number of challenges. This why make a lot of study written which based on cyberspace take part in legal and technique.

Alkaabi, Ali Obaid under the study of *Combating Computer Crime: An International Perspective* examined the approaches used for combating computer crime in Australia, UAE, UK and USA. This four countries represent a spectrum of economic development and culture. He said that, the global nature of the Internet has resulted enormously increased opportunities for the cyber criminals. Computer Crime or Cybercrime is increasingly becoming one of the main threats to the wellbeing of the nations of the world. Therefore, it clear that there is crucial need for common understanding of such criminal activity international to deal with it effectively. It is likewise very important to explore and understand the problem in detail and to identify obstacles to international cooperation in combating computer crime.

It is also important to identify and adopt best approaches for combating computer crime. He conclude that, is required to continued research into the extent to which

legislation, international initiatives, policy and procedures, and technology to combat and investigate computer crime are consistent globally and can be improved upon.[9] However, the Author look on what approaches to combat computer and cybercrime in developed Countries but the challenges also meet to developing countries like Zanzibar as a part of United Republic of Tanzania. The threat flow around the society since the number of computer user increased every day. Zanzibar identify the cyber problem and initiate a steps to take care on that problem by make amendment to her laws and established ICT policy as a running tool to prepare legislation to combat cybercrime. My study will analysis on legal documents that applied to stop cybercrime in Zanzibar.

Ozeren, Suleyman in his study *Global response to cyberterrorism and cybercrime: A matrix for International cooperation and vulnerability assessment*, he describe that [10]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, 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

[9]Alkaab, Ali, Combating Computer Crime: An international and Perspective, Oct 2010, Queensland University of Technology(http://eprints.qut.edu.au/43400/1/Ali_Alkaabi_Thesis.pdf (accessed 04th July 2014).

[10]Ozeren, Suleyman, Global response to cyber terrorism and cybercrime: A matrix for International cooperation and vulnerability assessment,digital.library.unt.edu/ark:/67531/metadc4847/m2/.../dissertation.pdf (accesses 28th June 2014).

technical, legal, political and cultural. Orezen study, identified variables that constructed the scale based on the expert opinion. Also, the study presented typology of cyberterrorism, which involves three general classification of cyberterrorism Disruptive and destructive information attacks, facilitation of technology to support ideology and communication, fund raising, recruitment.

The study response to the Zanzibar which require the supporting from Regional and International cooperation to prevent cyber crisis. Zanzibar have the chance to get high risk of cybercrime due to lack of legal measures and cooperation at the international level. My will observed which legal means are conducted to stop terrorist and cyber criminals in order to secure technical, political and cultural. The Orezen study will help the Zanzibar to classify cyber terrorism and to frame legal according to the classification.

According to Nyamaka, Daudi in the study of *Electronic contract in Tanzania: An appraisal of the legal frame work*found that firstly, the globe ecommerce transactions are increasing annually and unless a country (like Tanzania whose legal environment is behind the forces of technology) creates a requisite enabling legal environment in time it will miss the opportunities which electronic commerce avails to participants in the globe market. Secondly, since internet has become a channel of doing business belated legal responses will create uncertainty and expose participants to unnecessary risks. It is vital for the existing legal environment to respond positively to the needs of technology. It is predicted that countries that do not take time now to create appropriate infrastructures including legal environments, that supports internet will find their economies plummeting in a matter of years. His

further recommend that Parliament and executive agencies with power to enact laws and rules should be able to effect the changes in time because definite articulation of a legal position through a written code is a more preferable approach. [11]

Mollel, Andrew L. &Lukumay, Zakayo N., in study of *Electronic Transactions and The Law of Evidence in Tanzania* was found that, as ICT development necessitated changes in the way business transactions are currently conducted, the main challenge posed by these developments, in turn, is the necessity of parallel changes in both national and international legal framework to accommodation the changes. For the legislative process, two approaches are recommended. The first is to enact a comprehensive piece of legislation on ICT and electronic evidence to provide for admissibility of electronic records and documents as well as electronic signatures. It is proposed in this study that there should also be a specific statute to govern electronic signatures. This is because this area is very wide, and it needs special attention.

The second approach is judicial response. It is recommended that judges should continue to play a pivotal role in extending the existing principles governing paper-based documents and authentication to cover documents and signatures in electronic form. It is recommended that the judges should categorically hold that evidence in a computer hard disk flash disk; compact disk or floppy disk is relevant and admissible to prove or disprove a fact in issue in legal proceedings[12].

[11]Nyamaka, Daudi, Electronic Contracts in Tanzania: An Appraisal of the Legal Framework,2011,SAUT, Tanzania

[12]Mollel, Andrew L. &Lukumay, Zakayo N., Electronic Transactions and The Law of Evidence in Tanzania, 2007, IUC, Tanzania.

The two studies above from Nyamaka and with combination research of Mollel and Zakayo is 100 percent represent the situation of Zanzibar although the study wrote to focus Tanzania Mainland. Since we are the same countries also we have the same challenges. This study will look after the hardworking of Zanzibar Government to make the cyberspace free from crimes.

Minister for Information and Communication Hon. Rashid Seif Suleiman in his message when introduce ICT policy said that "The Revolution Government of Zanzibar recognizes the pivotal role of ICT sector towards the sustainable socio economic development; equally important is that ICT enabled development toZanzibar should be policy led, ensuring a better synergy between public and private sectors and alignment with national goals. This is the first time that a comprehensive ICT Policy has been elaborated to realize the vision of making Zanzibarknowledge based society. This policy document brings together the economic, social and political dimensions of our initiatives in the area of information and communication Technologies"[13].

Part 2 of Zanzibar e Government policy state that "It was noted that there are some clauses that recognizes the usage of electronic means in normal human life within Zanzibar legislation; however there is lack of consolidated and dedicated laws that foresee and promote the usage and the development of ICT in our daily lives; be it personally or officially. On the other hand; there is no authorized institution mandated to oversee overall ICT initiatives within the public sector".

[13]Zanzibar ICT Policy First Edition, June 2013

Mambi, Adam in his book ***ICT Law Book***; he said Tanzania has been slowly shifting her legal system to cope with globalization, economic and political reform. The development and innovation of technology that brought in the application of ICT around the world cause greatly impact to Tanzania. Generally the legal system in Tanzania is mainly based on common law principles. Regulatory steps to secure electronic transactions such as digital signatures, reforms to business laws, dispute settlement and others have not yet been promulgated.[14]

He overview about E-commerce and its legal implication at global level is Technology revolution was bring great changes which affecting the way of business is done. Also the way in which goods and several marketing ordered, and ways on which contracts are made and satisfied. This trend attitudes great challenges for the offline current laws in Tanzania and other countries which must needed to respond immediately to the developments on electronic transaction for high level which boost the economy.

Mambi explain that, the new style of electronic moneys transfer systems between financial institutions within or outside the countryobviously is not clearthat reflected by the legal framework that regulates financial transactions. For instance, the traditional method requirements of writing and manuscript signature which are not acceptable under electronic commerce. This are common features under such laws regulating and governing such business, But under digital technology the requirement of writing and signature is different to our current laws.In addition, he

[14]Mambi, Adam, ICT Law Book, 2010, MkukinaNyota, Dar es Salaam, pg13.

clarifies about the issue of legal implications of electronic security through electronic banking. The author describes that electronic banking in terms of legal issues is not addressed effectively through policies and legal framework of Tanzania. The current legislation in financial and other related business look like to be not suitable to electronic transactions. The laws that regulate negotiable instruments and Banking in Tanzania do not accommodate online transactions or payments of cyberspace rather than offline transactions.

CHAPTER THREE

3.0 RESEARCH DESIGN AND METHODOLOGY

.1. Introduction

This part is about the methodological issues showing how, when and what was done during the whole research processes. The part includes the area of the study, research design used to carrying out the study, type of the study, sampling and sample size, sampling frame and sampling procedure, methods of data collection and method for data analysis. The Materials of the study are collected from library and field research. It concerns critical assessment of the laws governing cybercrime practices in Zanzibar.

.2. Research Design

The study methodology is qualitative. The data obtained through interview of legal staffs and stakeholder to enable a suitable role in the study and analysed legislation documents to observed obstacles facing cybercrime law.

.3. Study Location

The study conducted in Zanzibar. The institutions included in the study are Director of Public Prosecution (DPP), High court of Zanzibar, Zanzibar Attorney General Chamber and Ministry of Constitution and Legal Affair, Zanzibar Law review Commission, Police Headquarter and MwembeMadema Police Station, Peoples Bank of Zanzibar,Zanzibar Telecommunication Company, Ministry of Infrastructure and Communication , The State University of Zanzibar (Department of ICT)

.4. Study Population

The population selected for study were Legal officers and ICT officer and technician at the different institutions available in Zanzibar. The selected one were responsible to make sure that daily activities performed through computer and related technology are safe.

.5. Research Instrument

The research instrument used in the study is the different legal document and include structured and unstructured interview. Interview was conducted to representative from the selected institutions mentioned above and stakeholders.

.6. Data Collection Method

For the purpose of this study, the data collected included secondary and primary data. Secondary data were collected from different published and unpublished records and other materials that were available through the internet and library such as textbooks, International and Regional Conventions, Constitutions and other Acts of the House of Representatives of Zanzibar, journals, periodicals, articles reports, newspapers and some other kinds of publications on matters relating to the subject. In Primary data the researcher collected the data through face to face interviews from legal officers and IT technician in Zanzibar Institutions.

.6.1. Field Research

This is performed under tools of research known as interviews and observations. Interview is selected as preferred tools for collecting data because it allow a discussion of the study and win to get details to clean and proving the hypothesis of

the study. The interview were semi structured because a question arise according to the discussion of the officers. The offices visited are DPP, high court of Zanzibar Attorney General chamber, Police, Ministry of Constitution and Legal Affair, Zanlink, PBZ and Zantel. At both office interview includes legal officers and ICT technician. Also observation as a part of research method have been took place in Police, Court and DPP office.

.6.1.1. Interview

Under this method of data collection, both structured and unstructured interviews were used in this study. The purpose of applying this approach was to collect sufficient information from the legal documents and respondentofficers in any form as deemed fit.

.6.1.2. Semi-Structured Interview

Semi structured interviews consist of several key questions that help to define the areas to be explored, but also allows the interviewer or interviewee to diverge in order to pursue an idea or response in more details[15]. In this study is used this type due to provides guidance to participants on what to talk in order to be flexible in elaboration of information needed.

.6.2. Library Research

In library research are conducted concentrated to find related materials as a primary data as well as secondary data materials for on cybercrime law in Zanzibar. These

[15]http://www.nature.com/bdj/journal/v204/n6/full/bdj.2008.192.html(accessed 18th July 2014)

reviewed materials were used in combining various parts of the dissertation and mostly testing the hypothesis of our study. Also used as bases in writing the research Background, literature review and statement of the problem.

The primary materials are extracted from legislation documents, magazines, leaders' speech, newspaper and policies. For secondary source includes textbook, cybercrime reports, journals and law cases. The libraries visited to collect a materials to complete the study are Zanzibar services Library, TheZanzibar University, The State University of Zanzibarand The Directors of Public Prosecution library.

CHAPTER FOUR

4.0 ANALYSIS OF ZANZIBAR LEGISLATIONS ON CYBERCRIME

4.1 Concept of Cybercrime and Cybercrime Law

In this section of literature review is to demonstrate a reader on what the researcher have read and a good comprehension of the main published work concerning on a particular study in the field. In this part, the researcher discuss on concept of cybercrime and cybercrime law, also look more for experienced of cybercrime around East Africa Community and International legal response.

4.1.1 Concept of Cybercrime

Cybercrime is a very global problem which affect every corner in electronic activities in our daily life. The unity of International, regional and local Governments is important to work together to fight against cybercrime or cyber terrorism. There unity have an advantage to avoid any danger which caused by internet, network or computer system in general. Because of the internet and computer life make the World as a village for communication thus criminals have no border to do their crime activities. The important things in cybercrime war is to remove obstacles of legal system inequalities of the states and law administration agencies.

The term cybercrime at present are common. And there are a number of definitions that agreed to state a cybercrime. For example

i. The use of any computer network or related for the purpose of crime (Source: British police).

ii. Any criminal offence committed against or with the help of a computer network (Source: Council of Europe).

These broad definitions offer little insight into the nature of the conduct that falls within the umbrella term. The issue is further complicated by the fact that cybercrime is a social label and not an established term within the criminal law. It seems that a situation has arisen in which everyone knows what cybercrime means but nobody can pinpoint exactly what conduct the term encompasses.[16] But in general we can defined as Cybercrime is defined as any criminal acts allocating a business with computer and network system or Cybercrime is an activities which includes both traditional and coming crimes which conducted through computer and internet for example Internet fraud, identity theft, and credit card account thefts are considered to be cybercrimes when the illegal activities are committed through the use of a computer and the Internet.[17]

According to the definition above, the activities such as theft of business and government information, website attacks or sending of virus problem and other computer illegal activities both include a cybercrime action. The good policy is the only way which organize stakeholder (Individuals, Governments and Services Provider) to solve this problem. The policy and legal strategic can bring the governments and responsible institution to set law and regulation to punish those deals with this unfair business. Increasing of communication network improve the online business such as electronic commerce, mode of sending information through

[16]https://www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf(accessed 17th July 2014)
[17]http://www.techterms.com/definition/cybercrime (accessed 02th July 2014)

emails and services and products advertisement. This improvement attract criminals to make more effort catch sensitive information or steal a business important codes.

4.1.2 Forms of Cybercrime Activities

Availability of cybercrime activities in our daily life carried out large impacts of threat to the Governments, individuals and business activities in the World. It clear that number of victims increase as well as improve communication technology, this improvement cause unfair situation like harassment, loss of money and high economic costs. The some of the costs of cybercrime can be measured compare to the value in terms of money. But others costs cannot measured in term of money it reflect directly to spread harmful to victims thinning out child abuse or stealing sensitive personal or Governments information. Criminals use the internet with high speed, easy encryption methods and sharing information to perform their crime and cause many challenges the target person or business. The aim of criminals is catch important or destroy data in order to gain benefit. The forms of cybercrime activities are hacking, theft of intellectual property, child grooming, stealing identity and sensitive data, computer and internet fraud and computer malware.

4.1.3 Intellectual Property

Intellectual property (IP) theft can be defined as a theft of material including commercial trade mark, patent and copyrighted materials like music, movies and books. Intellectual property crime uses the computer system to steal huge amounts of material that are copyrighted and cause damage to the victimized companies or individuals. Internet pirates target the online shoppers who look for discounted and

genuine products. They do so through emails and Internet advertisements where look to be the real thing. Consequence, individuals, companies, institutions which deals with education and even government agencies have been trapped by Intellectual Property pirates keen on buying stolen goods. The intellectual property cybercrime involved in crime in the form such as copyrighted material and trade/business secret. Theft of trade secret is the theft of ideas, technologies and information of industrial manufacturers, financial agency and computer industries. And theft of copyright material includes piracy of software, piracy of music or books. Theft of intellectual property affect economy of individual and governments because thieves sell pirated programs to a lot of user at cheap price and not pay revenue while the owner lost millions of money due to research and production plus tax payment.

4.1.4 Hacking

Computer hacking is defined as an activities that a criminal accesses a computer and network system without the authorization of the owner or controlling it to aim of theft or to use it as a way to do a crime for another person. Hackers usually are a very intelligent person can write a code/program to break computer or network system. Another way thinking and figure out password security of a user, he/she struggling to enter into system to do what plans to do. Also they decrypt the important information sent through internet like credit card especially in business which conducted online (electronic commerce) by keeping software to track every key and record their details.

Hackers after attacking and stealing of critical institution information such as business plans, customer details and other confidential issues leave a company to

suffer on loss. After attacking criminals may hawk information to other business competitor, also they make customer to shift from a company faced criminal problem to another company. Also hackers can spread a virus to the computer system and cause a lot of data to disappear. Many times website are attack by hackers and made to unavailable and causing trouble to user especially for business website. Another problems is hacker use someone identity for his/her interest like send a message to other through email.

4.1.5 Child Grooming

Child grooming is activities used to attract minors into deal of illegal businesses such as child prostitution and/or the production of child pornography. Child grooming involves actions purposely take on with the aim of helping and establishing an emotional linking with a child, to lower the Childs inhibitions in order to sexually abuse the child.[18] This is a behaviour that is typical have done of an adult who is sexually mostly attracted to children.

Adult may begin the grooming process by enter into social networking sites, at the chat rooms pages or interaction children through audio, video , email and text messages. The technologies in this days are simplify ways for criminal to contact with children through internet. Children are attracted online because they use computer on networking websites for social website or chat room. Criminals use false identities in chat rooms to attract Child and connecting and to be victim in the business of sexual abuse. Once this happen a child of online exploitation must live with their exploitation for the all the time of their lives.

[18]http://www.pandys.org/articles/sexualabusegrooming.html(accessed 01st July 2014)

4.1.6 Stealing Identity and Sensitive Data

This kind of crime occurs when a cybercriminal steals successfully personally identifiable information. This type of cybercriminal does not really benefit unless there is a financial reward for the effort or some type of damage that can be done with the data. Thus, identity theft serves as an access occur at opening or sending information of credit card, Purchasing goods or services through internet system, Renting or buying a house or apartment.

Sensitive data crime occurs when a cybercriminal gains an access to sensitive data and steals it in different ways such as unencrypted credit card information stored by a business, personally identifiable information, trade secrets, source code, customer information and employee records all attract the attention of cybercriminals. The crime can be as simple as copying things like customer data files in flash drive or other means and selling it to a competitor or using confidential material to compete with the other entity business.

The costs to victims of these types of cybercrime can be high, and involve both public damage and financial costs associated with loss of business, legal fees and cost of increasing security measures to defend theft.

4.1.7 Cyber Stalking

This is an activities use the email or other means of communication to communicate with others and cause harassment and/or threatening. This form takes a portion of offline stalking characteristics. It is growing a serious problem because it not a physical contact and may create a problem of misperception.

The crime of stalking has existed for decades, stalking refers to repeated harassment of someone where the stalker acts in a threatening behaviour toward the victim. Threatening behaviours include following the victim, appearing at the victim place of work or near his or her home, then making eye contact so the victim knows someone is following, and leaving threatening messages on paper or the telephone. Stalking leaves its victims fearful of bodily harm or death.[19]

4.1.8 Computer and Internet Fraud

Computer fraud as the use of a computer to create a dishonest misrepresentation of fact as an attempt to make another to do or refrain from doing something which causes loss. This criminal are done by different number of activities. First, they can alter computer input in an unauthorized way, for example Employees may cheat company funds by altering input data. Second, criminals can be change and/or delete stored data. Third, sophisticated criminals can rewrite software codes and upload them into a bank's mainframe so that the bank will provide its user identities to the thieves then thieves can use this information to make unauthorized credit card purchases.[20]

These crimes are using by computers and/or Internet services to defraud people, government, companies and agencies of money. There are many methods used to perform these illegal activities like Phishing, viruses, and Distributed Denial of Service (DDoS) attacks are fairly well known strategies used to disturb service or gain access to another funds.

---

[19] http://law.jrank.org/pages/11992/Cyber-Crime-Intellectual-property-theft.html,(accessed 01st July 2014)

[20] http://www.law.cornell.edu/wex/computer_and_internet_fraud,(accessed 12th July 2014)

4.1.9 Computer Malware

Viruses and worms are all in same class of software called malware. It is specific code or software that is designed to cause damage, interruption, steal, or in general do bad action on data, hosts, or networks.[21] Today the Internet is the biggest source of computer viruses. Email viruses and Worms have become more common ways of spreading viruses.

Virus: Computer viruses is a computer program which attached themselves to other programs in computer system like Microsoft word, spreadsheets or games. When these programs spreading to computer system the virus code is effect and performs a task like duplicating itself and infecting other computer programs and files by harmful things like corrupt or erase data of a computer system.

Viruses spread throughsharing of flash discs and files which were popular to share programs. For example Trojan horse viruses are hidden computer program without the user knowing sometime can be used to make it easier to hackers to get into a system because can look like a login screen. For example if launched Melissa virus will attempt to start Microsoft outlook to send copies of the infected documents via email to up to 50 people in outlooks address book as an attachment..[22]

Worms: Computer worms are alike to viruses in that they duplicate functional copies of themselves and can cause the same type of damage. In difference to viruses, which need the spreading of an infected host file, usually are standalone software

[21]http://www.websitedefender.com/what-is-malware/,(accessed 06th July 2014)
[22]http://www.melissavirus.com, (accessed 2nd July 2014).

and do not require a like host program or human assistance to circulate. A worm enters into a computer through a weakness in the system and takes advantage for file or information transport features on the system.

4.1.10 Concept of Cyber Law

Cyber Law is a rapidly evolving area of civil and criminal law as applicable to the use of computers, and activities performed and transactions conducted over internet and other networks. This area of law also deals with the exchange of communications and information thereon, including related issues concerning such communications and information as the protection of intellectual property rights, freedom of speech, and public access to information.[23] According to the laws for cyberspace an acts have been known and classified as cybercrimes. There are some techniques set for investigation of cybercrime and there are adjudging authorities or court of law established in order to hear and organise these cases of cybercrime.

Investigations into cybercrimes can be done through Computer Forensics and Time Stamping. Computer forensics is the process of Identifying, Procuring, Analysing, & Presenting Digital Evidence in a manner that is legally acceptable in the court of law. Computer forensics is used to conduct investigations into computer related incidents whether the incident is an external intrusion into your systems, internal frauds or staff breaching your security policy. The most important factor in the investigation of cybercrimes is to prove the "Time" of the occurrence of the crimes, as time stands to be most important factor in computer forensics it is very important. Under the

[23] http://definitions.uslegal.com/c/cyber-law, (accessed 2nd July 2014).

concept of time stamping crimes are synchronized as events of an accurate clock. In the case of cybercrimes it is almost impossible to commit a crime without leaving a time trail. The results of the time stamping are regarded as to be as undisputable evidence. Time stamping speeds up the investigation and dissuades the cyber criminals.[24]

4.1.11 The Group of Offences in Cybercrime

In law enforcement, cyber offences can be divided into three groups. The groups are known as offences where the computer as a target of a crime, offences where the computer is the tools to commit the crime, and offences where the computer is the repository of evidence of crime. In this part of study would examine the difference on each group.

Edward Carter in his article called *"Examining Cybercrime: It forms and it's Perpetrators"*state the nature of offence in cybercrime as:

4.1.12 Computer as Target of crime

In this group of offence, the purposes of criminals is not to steal an information stored in computer or software obtained in it but their aim is change the data or programs contained in victim computer. The good example this offences is to planting a virus to target computer. Denial of services attacks included in this type of offences. In this example, Criminal directs a numbers of messages to a victim computer system so that victim are unable to access it. Good example is in business operation attack where criminal accesses a network system of the company control

[24]http://aspireip.com/cyber-crimes-space-and-so-forth-a-concept-of-cyber-laws/,(01st July 2014).

delivery and destination of customers and business information. These crimes usually not involved for the purpose of financial gain but most of time involved for disrupting operation of business or government. It cost a lot of money to recover the system after every hour.

4.1.13 Computer as Tool to Commit an Offence

Another group of cybercrime offence is the traditional offences committed by using computer as a tool. Usually these traditional offenses include crimes such as embezzlement, forgery, theft, or gambling. A strong argument can be made that when these types of offenses are committed with the use of a computer they are not cybercrimes at all and should, in fact, be considered as nothing more than traditional crimes committed by a different means. Murder is classified as murder without regard to the means used to commit it, and there does not seem to be a strong reason to think of a traditional crime such as forgery as being different just because a computer is used to commit it.

The cybercrimes in this group are the most frequently committed types of cybercrimes. In some instances the crime committed with the computer may not, for technical or other reasons, fit within the statutory definition of a traditional offenses even though the result brought about by the use of the computer is clearly within the concept of a traditional criminal statute. Thus, whether forgery committed with a computer includes the making of a false electronic record may depend on how the term “document” is defined in the a forgery statute and whether using a computer to steal data or trade secrets constitutes theft will depend on whether the term

"property" in a theft statute includes intangible property.[25]

4.1.14 Computer as Repository of Evidence of a Crime

The third offense group of cybercrime consists a computer is a repository of evidence for the type of offense. An example of this category of cybercrime is the drug dealer who, like any legitimate businessman, keeps his financial records and customer lists in a personal computer, tax evasion where the perpetrator is engaged in a legal business but evades taxes and keeps his true business records in an electronic format. Analytically, it seems incorrect to classify almost any of these types of offenses as cybercrimes because, with the exception of those cases such as child pornography where mere possession of the electronically stored image is a crime, a computer is not involved in their commission.[26]

According to Edward Carter, Repository offences apply challenges to law enforcement on which how acquire the electronically stored evidence. But the advice to avoid the problems is investigations will perform only for data in the computer rather than the computer itself.

4.2 Current Legal Responses to Combat Cybercrime

Legal actions play a major key role in to prevent and combating of cybercrime. in order to reduce the cybercrime problem law is must be dynamic tool that can enables the states to respond to any kind of criminal, new cybercrime challenges and maintain security. For best result national laws and international laws both must covers laws that are related to cybercrime. The common current laws was setup to

[25] www.univd.edu.ua/_projects/ezloch_kor/docs/eng/37.doc, (accessed 11th July 2014)
[26] Carter, E, *Examining Cybercrime: Its Forms and Its Perpetrators*, 2002, NUIA, Kiev

fight with cybercrimes are:

4.2.1 Data Protection Act

The Data Protection Act 1998 (DPA) was passed by United Kingdom Parliament. This is designed to protect a data stored on computers. The aim to handle and control information and give legal rights to those have information stored and how people can be used it. The Act set a basic way such as setting rules that can be follow by people and companies that deals to store people information. The Act is work by setting rules of Information Commissioner have power to enforce the Acts and Data controller that keep and collects Data about people For example Customer Information. The office Information Commissioner apply great role to make sure that society are obey the rules in order to prevent a misuse of Data.

The act controls how personal information can be used either business, organization or Government. And want responsibilities to everyone using data to follow strict rules of information which must be used fairy and lawfully, limited, specifically stated purposes, accurate, not keep longer than necessary, must be safety and secure. And legal protection for sensitive report like political, religious, health, criminal reports.

4.2.2 The Computer Misuse Act (1990)

This Act was passed by United Kingdom Parliament that protect certain illegal activities like hacking, software misuse or someone help another to get access to protected files of the others computer system. This very example act that came to protect a cybercrime because is created after the 1984-1985 case of R and Gold.

The UK computer Misuse Act created three categories offence to combat cybercrime. These are:[27]

1) Accessing computer material without permission, For example looking at someone else's files. a) there must be intent to access a program or data stored on a computer, and the person must know that this access is not authorised (b) This is why login screens often carry a message saying that access is limited to authorised persons: this may not prevent a determined and ingenious hacker getting access to the system, but they will not be able to claim ignorance of committing an offence.

   This offence punishment is six months imprisonment or £5000.

2) Accessing computer material without permission with intent to commit further criminal offences: for instance accessing personal files or company records in order to commit fraud or blackmail. For example crime for bank system and wanting to increase amount in his/her account. This punishment by six months or maximum fine or 5 years or fine.

3) Altering (modification) computer data without permission, for example writing a virus to destroy someone else's data, or actually changing the money in an account. Also this punishment as section 2 offence.

4.2.3 Copyright Law

The United Kingdom is established the Copyright, Design and Patents Acts 1998 and extended the rules covering a work of Computer programs. The Acts prevents

[27] http://www.doc.gold.ac.uk/~mas01rk/Teaching/CIS110/notes/Computer-misuse.html, (accessed 05th July 2014).

the software piracy by giving owner a right to control, sell and distribute their work safely. The works that prevented by this Act are like Books, Video and computer software. For the reference of the law, is forbid for those who buy software by (a) to give a copy to their friends (b) produce a software copy and selling (c) using software to network if the licence is not for network licence (c) renting software without the permission of the holder. The law introduce a penalties for copyright infringement criminal such as £5,000 or/and imprisonment six months before magistrates court and unlimited fine up to ten years imprisonment in the Crown Court.

According to the copyright law software companies have rights to stop piracy by take many steps such as the licence agreement between the company that developed software and user and covers copyright. And must be agreed before the installed software, Companies give a unique key licence to the software and enter to confirm the licence right during installation and/or Software application run if machine plug to internet after user install supporting file of the software. For more effort to combat the software theft, The Federation Against Software Theft (FAST) was founded in 1984 by the software industry and is now supported by over 1,200 companies. It is a not-for-profit organisation with an aim to prevent software piracy and has a policy of prosecuting anyone found to be breaching copyright law. FAST also works to educate the public about good software practice and legal requirements.[28]

[28]http://www.bbc.co.uk/schools/gcsebitesize/ict/legal/2copyrightrev1.shtml, (accessed 03rd July 2014).

4.2.4 The OECD Guidelines For the Security of Information Systems and Networks

This guidelines are released by the Organisation for Economic Cooperation and Development (OECD) at September 2002.The guidelines is provided in order to develop security and privacy for member countries in Digital World. These guidelines apply to participants in the information system and network that build awareness and understanding of security subjects in the Digital worlds and the following are guidelines that constitute a foundation for work towards a culture of security throughout society.[29]

1. **Awareness:** Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. **Responsibility:** All participants are responsible for the security of information systems and Networks.
3. **Response:** Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
4. **Ethics:** Participants should respect the legitimate interests of others.
5. **Democracy:** The security of information systems and networks should be compatible with essential values of a democratic society.
6. **Risk assessments**: Participants should conduct risk assessments.
7. **Security design and implementation:** Participants had better incorporate security as an essential elements of information systems and networks.
8. **Security management:** Participant should adopts a comprehensive approach to a security managements.

[29]http://www.oecd.org/internet/ieconomy/15582260.pdf,(accessed 07th July 2014).

9. **Reassessment:** Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures

The guidelines were to the member countries. This help them to design laws that can be used to make better security of their computer and network system , Also the guidelines alert individuals users to be aware and responsible and take preventive measure in their daily activities which concern with computer, network and internet connectivity.

4.2.5 The Deauville Declaration for Internet

In 26 May 2011 G8 countries established Deauville Declaration for Internet said that "Their implementation must be included in a broader framework: that of respect for the rule of law, human rights and fundamental freedoms, the protection of intellectual property rights, which inspire life in every democratic society for the benefit of all citizens. Strongly need to believe that freedom and security together with transparency and respect for confidentiality as well as the exercise of rights and responsibility have to be achieved all together. Both the framework and principles must receive the same protection, with the same guarantees, on the Internet as everywhere else".[30]

The objective of this declaration is to harmonizing the computer and cybercrime laws to prevent the emergence of safe to put for cybercriminals. It recommended that

[30] Section II (10) , G8 Deauville Declaration: INTERNET

the creation of laws and fighting of criminals must be work together to achieve the goals.

4.2.6 Resolution by the Commission on Crime Prevention and Justice

A draft Resolution 65/230 proposed by the Commission on Crime Prevention and Criminal Justice (CCPCJ) in Article 8 was based on the Salvador Declaration Article 42 (2010) of the United Nations. This Resolution of CCPCJ made a suggestion to establish as follows: " an open-ended international expert group to conduct a broad of the problem of cybercrime and responses the results to it by the Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime."[31]

The General Assembly in the Thirteenth Congress will focus on "Integrating crime prevention and criminal justice into the wider United Nations agenda to address social and economic challenges and to promote the rule of law at the national and international levels, and public participation".[32] This UN concentrating on the cybercrime problem which growing due to the increasing of Internet users and criminals get greater opportunities to catch new children and women to criminal, harassment and sexual abuse. The UN take action to combat crime plus promote the

[31]General Assembly resolution 65/230
[32] resolution 67/184, CCPCJ

role of criminal law to prevent illegal trafficking, crime prevention and improve the efficiency and equality of criminal justice systems international.

4.2.7 Child Exploitation and Online Protection Centre

The Child Exploitation and Online Protection Centre (CEOP) is established in United Kingdom and UK National Crime Agency (NCA) is responsible to the child right under this legal project. This is stand to work inside the UK and internationally in order to make online sites are safe place children and protect any involvement of child abuse resources.

In Lanzarote October 2007, European Union members sing a treaty of Protection of Child against sexual Exploitation and Sexual Abuse, this make another legal tool that used to combat Children against Sexual Exploitation and Sexual Abuse. According to this treaty, this Convention is the first instrument to establish the various forms of sexual abuse of children as criminal offences. Preventive measures outlined in the Convention include the screening, recruitment and training of people working in contact with children, making children aware of the risks and teaching them to protect themselves, as well as monitoring measures for offenders and potential offenders.

The Convention also establishes programmes to support victims, encourages people to report suspected sexual exploitation and abuse, and sets up telephone and internet helplines for children. It also ensures that certain types of conduct are classified as criminal offences, such as engaging in sexual activities with a child below the legal

age and child prostitution and pornography. With the aim of combating child sex tourism, the Convention establishes that individuals can be prosecuted for some offences even when the act is committed abroad. The convention legalises those who enter into business of children for sexual purposes grooming and sex tourism. The new legal tool also ensures that child victims are protected during judicial proceedings, for example with regard to their identity and privacy.[33]

4.2.8 Convention Against Transnational Organized Crime (TOC)

The United Nations release a Convention Against Transnational Organized Crime which concern on stopping of cybercrime activities among the member states. This came due of the result of news report on cybercrime have been touched headlines of Media daily. According to the U.N convention offences are done their crime by involve organized criminal groups International and are committed to achieve an important material or financial benefit include a sexual enjoyment. The objective of United Nations is set protocols to prevent, destroy and plan punishment in trafficking in those people deals with children exploitation and Women abuse together with misuse of Information Technology devices and system.

Because organized crime and corruption often go hand in hand, the U.N. Convention against Corruption could also be useful in breaking up online child exploitation rings. While the Convention on the Rights of the Child (CRC) does not explicitly prohibit online child abuse, the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography could

[33]http://conventions.coe.int/Treaty/EN/Summaries/Html/201.htm, (accessed 08th July/2014).

give states points to set out policy on this problem which is in the best interests of the children.[34]

4.2.9 The Computer Related Crimes Act

The model law, titled the Computer Related Crimes Act was adopted by common wealth in 2002, this is the effort to fight the cybercrime among the member states. The model law work for a common principles that each State can use to approve framework legislation well matched with other Commonwealth States. To keep effort on Third World countries on that serious problem the Commonwealth introduce a training programme which conducted at Malta at June 2009, the training was on Legal Frameworks for Information and Communication Technologies. This training course aimed also to provide an understanding of emerging matters and present international dialogue on subjects such as Broadcasting and Interconnection, Internet Governance, Cybercrime and Jurisdiction.

4.2.10 European Cybercrime Centre (ECC)

The establishment of the European Cybercrime Centre is introduce for the development to fight against cybercrime. The ECC help the Union member governments, businesses and citizens to have the tools to tackle cybercrime and make the Europe cleverer and stronger in its fight against cybercrime and fast to solve any problem occurred. The European Cybercrime will work for as the Centre of European information on cybercrime. The centre support investigation, building capacity to struggle on cybercrime through working out, awareness educating and

[34] http://www.peacepalacelibrary.nl/2013/10/protecting-children-from-cybercrime-online-child-grooming/(accessed 07th July 2014)

providing best practice on cybercrime. Moreover, the Centre will build experts community for all sectors of society to battle and stop cybercrime and online child sexual exploitation.

The EU, works with EU stakeholders, non EU countries, international organizations, internet governance bodies and service providers, companies involved in internet security and the financial sector, academic experts, civil society organisations, National Computer Emergency Response Teams. And forming a safer Communication information around the world by improve and maintain the high security of information infrastructures and combating any computer activities related crimes, the European Union set four principal points must be existing in any cybercrime policy are:[35]

1. The adoption of adequate, substantive, and procedural legislative provisions to deal with both domestic and transnational criminal activities;
2. The availability of a sufficient number of well-trained and well-equipped law enforcement personnel;
3. The improvement of the cooperation between all stakeholders, users and consumers, industry, and law enforcement; and
4. The need for ongoing industry and community-led initiatives.

4.2.11 The Council of Europe Convention on Cybercrime

The council of Europe Convention on Cybercrime was released for sign in November 2001 and move into force in July 2004. Allow member and non-member

[35]https://www.europol.europa.eu/sites/default/files/publications/ec3_first_year_report.pdf, (accessed 02th July 2014).

states to sign the treaty and to be only International Treaty Binding on the subject of Cybercrime. It represents guidelines for International wishing to develop security, legislation, ways to protect freedom and human rights against cybercrime. This is good idea for Council of Europe to allow a non-member states to join because it provides a framework of international cooperation to solve criminal problem in this digital world. The effective rules and protocol are established by convention to allow everybody to join and avoid no body to own demanding task of that problem. The rules minimize the risks and maximise right and freedom across cyberspace and remove intolerant nature committed through computer system.

Communication technology develops more rapidly than the response of legal action. There is need to address a lot of challenges frequently associated to data protection, for example fighting online child abuse, law of public and private deals of sharing information. To make safe Internet for Child in 2011 the council of Europe and the Virtual Global Task Force signed a cooperation agreement to fight and protect online Child abuse. European Union make a great effort to harmonize laws that prevent a child pornography and child exploitation.

The Council of Europe Convention on Cybercrime aimed is to protect society from cybercrime in general including child pornography. In Content-related offences, this article concern on Offences related to child pornography “child pornography seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernising criminal law provisions to the more effectively circumscribe the user of computer systems in the commission of sexual offences

against children". [36]

The effect of this convention is to stop for any purpose child pornography like distribution, the offering or making available, the procurement on or through a computer system. The goals of Convention are to protection of society against cybercrime by providing sufficient powers for combating cybercrimes by supporting crimes investigation and detection. Also providing consistent international cooperation and assist trial for offences of criminals in both levels local and international.

According to the Budapest Convention on Cybercrime there are three Principal Parts in this Convention. The first part harmonizing the domestic criminal substantive law elements of offences and connected provision in the capacity of cybercrime. An Agreement needs Parties to accept such law-making and additional events that necessary to establish as criminal offences under its local law, when committed on purpose such as the access to the full or any portion of a computer system without right, the production for the purpose of distribution, the offering or making available the distribution or transmission, the procurement, or the possession of child pornography on or through a computer system, determine breach of any copyright when done on a commercial by means of a computer and network system.

The second, Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidences in relation to which is in

[36]The Council of Europe Convention on Cybercrime, Article 9.

electronic form.This part of the Convention requires Parties to decree confident technical methods and procedures to simplify the investigation of cybercrimes or any part of computer crimes for which evidence and confirmation may be bring into being in electronic form. This part preservation of specified computer data, including traffic data that has been stored by into computer system. The third part, setting up a fast and effective regime of international cooperation. This Parties, introduce cooperation with each other to the widest possible level for the aim of investigations or measures concerning criminal breaches connected to computer data and network systems, or for the gathering of evidence in performed in electronic system of a criminal faults.[37]

4.2.12 Cybercrime Legislation East Africa Community

According to workshop report on effective cybercrime legislation in eastern Africa conducted in Dar es salaam, Tanzania, 22-24 august 2013 presented by Mr. Patrick Mwaita and Mr. Maureen Owor, 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 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.[38]

---

[37]Vatis, Michael , The Council of Europe Convention on Cybercrime, https://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf(accessed 03rd July 2014)

[38]Patrick Mwaita And Maureen Owor (Accp),Workshop Report on Effective Cybercrime Legislation in Eastern Africa Dar es Salaam, Tanzania, 22-24 August 2013.

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.[39]

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 hosts 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[40].

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

[39]Mwaita, Ibid, pg 9
[40]Mwaita,Ibid, pg7

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 analyse 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.[41]

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 unauthorised use, access, abuse of computers or data. It also has provisions on electronic fraud, child pornography, and cyber harassment, cyber-stalking. The Electronic

[41]Mwaita,ibid,pg 8

Transactions Act provides for the use, security, facilitation and regulation of 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.[42]

Cybercrime is relatively new in Burundi. Although there is no specific legislation to criminalise 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 behaviours 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 unauthorised 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 elements.[43]

4.3 Analysis of Zanzibar Legislation to Combat Cybercrime

Document analysis is used as a tool in this study. A document is something that we can read and which relates to some aspect of the social world. Official documents are

[42]Mwaita,ibid 10

[43]Patrick Mwaita And Maureen Owor (Accp),Workshop Report on Effective Cybercrime Legislation in Eastern Africa Dar es Salaam, Tanzania, 22-24 August 2013.

intended to be read as objective statements of fact but they are themselves socially produced.[44] Document analysis is a form of qualitative research in which documents are interpreted by the researcher to give voice and meaning around an assessment topic. Analysing documents incorporates coding content into themes similar to how focus group or interview transcripts are analysed.

A rubric can also be used to grade or score a document. There are three primary types of documents which known as Public Records: The official, ongoing records of an organization's activities. Examples include student transcripts, mission statements, annual reports, policy manuals, student handbooks, strategic plans, and syllabi; Personal Documents: First-person accounts of an individual's actions, experiences, and beliefs. Examples include calendars, e-mails, scrapbooks, blogs, Facebook posts, duty logs, incident reports, reflections/journals, and newspapers; Physical Evidence: Physical objects found within the study setting (often called artefacts). Examples include flyers, posters, agendas, handbooks, and training materials.[45]

4.3.1 Legal Documents to Combat Cybercrime in Zanzibar

The Revolutionary Government of Zanzibar made several initiatives in development of ICT sectors and to improve information service delivery to the public as well as initiating laws to prevent cybercrime. There are some legal documents in Zanzibar recognizes the importance of ICT. For the existing laws do not satisfy for the whole field of ICT application in government, business and other socio-economic aspects.

[44]http://www.drcath.net/toolkit/document.html,(accessed 28th July 2014)
[45]http://studentresearch.ucsd.edu/_files/assessment/Assessment-Methods.pdf, (accessed 05th July 2014).

Also there is some comprehensive and relevant acts which recognize legal acceptance of electronic technology.

4.3.2 Zanzibar Penal Act No.6 of 2004

This is the greatest comprehensive and probable Act in prosecution which is concern with whole procedures to attain the offence with its ingredients and punishment for the offences. In

Parts XXXIII it outlines penalties on offence of computer equipment and related or supplies. Offences[46]:

> *Any person who wilfully, knowingly, and without authorization modifies data, programmes, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offence.*[47]
>
> *Any person who wilfully, knowingly and without authorization destroys data, programmes, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offence.*[48]
>
> *Any person who wilfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offence.*[49]

[46]Zanzibar Penal Act No.6 of 2004,S.373
[47]See section 373(1),Ibid
[48]See section 373(2),Ibid
[49] See Section 373(3),Ibid

Also the Act identify the offence on Destruction of Computer equipment. The destruction of computer is the one among the crime performed either by destroying the information Business or to put on hiding evidence.

> *Any person who wilfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits an offence against computer equipment or supplies, and is liable on conviction to imprisonment for a term of not exceeding five years. If the offence is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony and is liable on conviction to imprisonment for a term not exceeding ten years.*[50]

In sect 375 and 376 of the Act state offence on Interfering with data and Computer System. This section liable those who interfere by destroying or damage Computer system and data without the authorization of owner.

> *Any person who wilfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever wilfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offence against computer equipment or supplies, and is liable on conviction to imprisonment for a term not exceeding ten years*[51].

[50] See Section 374(1),Ibid
[51] See Section 375(1),Ibid

The Act provided that if the damage to such computer equipment or supplies or to the computer, computer system, or computer network is Tsh. 1,000,000 or greater, or if there is an interruption or impairment of governmental operation or public communication or other public service, then the offender is guilty of a felony and is liable on conviction to imprisonment for a term not exceeding fifteen years.

Other offences stated in Act are Illegal Interception of data:

> *A person who intentionally or recklessly, without lawful excuse or justification: (a) hinders or interferes with the functioning of a computer system; or (b) hinders or interferes with a person who is lawfully using or operating a computer system; commits an offence punishable, on conviction, by imprisonment for a period not exceeding five years or a fine not exceeding five hundred thousand shillings or both. In subsection (1) "hinder", in relation to a computer system, includes but is not limited to: (a) cutting the electricity supply to a computer system; and (b) causing electromagnetic interference to a computer system; and (c) corrupting a computer system by any means; and (d) inputting, deleting or altering computer data.*[52]

Andsection 378(a)(b)(c)(d)stated on illegal device about the person intentionally without lawful excuse or justification interferes an operating computer system and corrupting, delete or change Computer Data. Therefore another offences stated in the Actisagainst computer users in section 379 where a person's commits an offence if

[52]See Section sect. 377(1) (a)(b)(c)(d), ibid

intentionally make available of computer program that is designed or adapted for the purpose of committing an offence. The offences about Fraud and related activity on Government computers in the Act stated as.

> *Any person who wilfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever wilfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offence against computer users, and is liable on conviction to imprisonment for a term not exceeding five years. If the offence is committed for the purposes of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony and is liable on conviction to imprisonment for a term not exceeding ten years*[53].

4.3.3 Zanzibar Criminal Procedure Act No.7 of 2004

This Procedure Act is very important in criminal prosecution and investigation, a number of offences which provides for the techniques on how to investigate and take legal action to a certain offence so as to get belief of a case. The Act in the section 136[54] outlines the procedures for searching and seizure of the computer data as:

> *If a magistrate is satisfied on the basis of information on oath that there are reasonable grounds to suspect that there may be in a place a thing*

[53]see section 380, ibid
[54]Zanzibar Criminal Procedure Act No.7, 2004.

or computer data:

(a) That may be material as evidence in proving an offence; or (b) That has been acquired by a person as a result of an offence; the magistrate may issue a warrant authorizing a police or any authorized person to enter the place to search the thing or computer data.[55]

In this section "thing" includes: (a) Computer system or part of a computer system; and (b) A computer data storage medium. [56]

Also the Act provides that if any kind of assistance needed as to searching the person who is the possessor or controller of the computer data media or computer system, may provide assistance by obtaining a copy of computer data, using equipment to make copies and obtain an intelligible output from computer system in a plain text format that can be read by a person.

In this section "assist" includes providing passwords, encryption keys and other information necessary to access a computer or computer system[57].

Also the act in section 139 give more details about criminal investigation to satisfied computer data.

If the Director of Public Prosecutions is satisfied that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings he may, by order in writing that:

---

[55] See Section 136(1),Ibid
[56] See Section 136(2),Ibid
[57] See Section 137(3), Ibid

> *(a) a person in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; and (b) an internet service provider or other service provider produce information about persons who subscribe to or otherwise uses the service.*[58]

4.3.4 The Employment Act No. 11 of 2005

This Act applies to all employment in the private and public sector. It establishes confidential to information by the employee in discharge of his/her duties. The Government of Zanzibar made several initiatives in development of ICT to improve service delivery to the public. This Act prohibited any employee to disclose a Government confidential information.For example the Act state that:

> *A labour officer or inspector shall in the exercise of his or her functions observe strict confidentiality and shall not divulge any information obtained in the course of his or her work in terms of this Act except if the information is disclosed in compliance with the provisions of any law: (a)to enable a person to perform a function or exercise a power in terms of an employment law; (b)for the purposes of the proper administration of this Act; (c) for the purposes of the administration of justice*[59].

This section ensure employees to keep confidential information of the office in safe manner.

---

[58]See Section 139, Ibid
[59]The Employment Act No. 11,2005,S. 20

4.3.5 Public Services Acts No.2 of 2011

This act outline issues about Record and Information Management and Public Services Management Information Systems. The Act mention that the Central Office is responsible for public records management and for the application, operation and management of information and communication technology in the public service and therefore execute the information for the purpose of ensuring that records management and information and communication technology are key springs to the efficient and effective of a public services. This promote the use of information and communication technology in organization to enhance the efficiency of their development and administrative operations and not deliver the information to criminal.

In section 96 of the Act lead the Head of institution to ensure that the data is secured and proper useful.

> *(a)Acquire and use information and communication technologies in a manner which (i) leverage economic of scale; (ii) ensure the interoperability of its information system with information system of other institutions if it is so necessary so that to enhance efficiency or services delivery; (iv) ensure security of its information systems.*[60]

The Act is very important for moral reasons and human right in order to secure and uses of information for specific need.

[60]Public Services Acts No.2 of 2011,S.96(4)

4.3.6 Prevention of Terrorism Act (URT) of 2002

For fighting Terrorism, The Act is applied for the United republic of Tanzania. Its aim is to protect the country on terrorist. The law established to prevents terrorist activities and a mechanism through which Tanzania can cooperates with Regional countries and Internationalin fighting on criminal. In this act specifically talks on terrorism act by conducting disruption in computer system, communication infrastructure and banking services.

> *(g) is designed or intended to disrupt any computer system or the provision of services directly related to communications infrastructure, banking or financial services, utilities, transportation or other essential infrastructure;*[61]

Terrorist most of the time organise and operate their criminal successfully due uses of Internet, computer and network system in their communication. The law prevent ability of terrorist to send a money from into or passing through Tanzania as a border.

4.3.7 Copyright Act No.14 of 2003

This is an Act that protect cybercrime. It mentions computer program as one among the works to be protected under copyright. This deals with infringement of intellectual property rights for those committed offence which concern both of copyright holders and those who work professionally with computer. The copy and distribution of the computer protected works without the approval of the copyright holder are very frequent. In part II of the Act[62] state the Copyright work as.

---

[61]Prevention of Terrorism Act (URT),2002,S.4(3)
[62]Copyright Act No.14 of 2003

> *Literary, and artistic works (hereinafter referred to as "works") are original intellectual creations in the literary, artistic and scientific domain, Including In particular: a) books, pamphlets, Computer programs, scientific or artistic writings and other writings.*[63]

The Act protect copyright because these days it have been done ease with unauthorised copies, due digital technology and copy and distribution it made easy through electronic network.

4.3.8 Anti-Money Laundering

Money laundering is the engagement of a person or persons, directly or indirectly in conversion, transfer, concealment, disguising, use or acquisition of money or property known to be of illicit origin and in which such engagement intends to avoid the legal consequence of such action. It is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the proceeds of crime. In essence money laundering seeks to achieve two basic goals: the first one is to separate the perpetrator and the proceeds from the underlying crime/predicate offence while the second is to disguise the proceeds as legitimate funds or assets and hence allow the criminal to enjoy the benefits of criminal activities[64].

The Internet is the one among the opportunities taken for cybercrimetoorganized crime that launder their criminal over computer networks system.The reasons why criminals want to launder money is the money is evidence of crime and inorder to

[63] See Section 3(1), Ibid
[64] URT, Strategy for Anti-Money Laundering and Combating Terrorist Financing, July 2010 June 2013.

hide legitimate income to avoid income tax in countries which levy income tax[65]. Placement of dirty money into financial system involves a series of transactions by transferring the money local or offshore banks as a payment or loans. Since the banks in this days are work online criminals have an opportunities to send their money easily if there is no cyber laws to protect them.

In Zanzibar, the Anti-Money Laundering and Proceeds of Crime Act No. 10 of 2009 state steps that followed to verify customer identify.The Act allow placing Under surveillance for the purpose of obtaining evidence of the serious or money laundering offence under this Act, a police officer of the rank of Assistant Superintendent of Police, after being authorized in writing by the Director of Public Prosecutions:

> *(a) have access to computer data, systems, networks and servers; (b) place under surveillance, tapping of telephone lines, facsimile machines or electronic facilities; (c) make audio or video recording of acts and behaviour or conversations; (d) have access to notarial and private deeds, or financial records*[66].

Also, the Act mention the requirements taken for identification. This will help to protect cybercrime because criminals usually hide their true identity when conduct their crime through internet or network system.

> *A reporting person shall take reasonable measure to satisfy himself as to the true identity of any applicant seeking to enter into a business relationship*

[65]Alkaab, Ali, Combating Computer Crime: An international and Perspective, Oct 2010, Queensland University of Technology, http://eprints.qut.edu.au/43400/1/Ali_Alkaabi_Thesis.pdf (accessed 04th July 2014).
[66]The Anti-Money Laundering and Proceeds of Crime Act No. 10,2009, S.85

with him or to carry out a transaction or series of transactions with him, by requiring the applicant to produce an official record reasonably capable of establishing the true identity of the applicant[67].

4.3.9 Zanzibar Evidence Decree

Any computer technologies and other related digital technology is the result of revolution and development of Information Communication Technology. The Technologies change Zanzibar society to modern life as other society in the world. The electronic medium, similar to the physical medium, creates many opportunities for the commission of crimes, such as hacking phishing, identity theft, and online child pornography, cyberstalking, creating viruses, unsolicited emails, and distributed denial of service attacks among many others. When a crime is committed, one of the parties in the subsequent criminal proceedings may wish to rely on information generated, distributed or stored on electronic devices such as spreadsheets, emails, text messages, databases and traffic data.

Arguably, the current digital technologies and the evolution of communications systems including e-commerce have substantially transformed the process of exchanging information, data and products, services in all spheres of human life such as business, civil, social and education and have indeed increased the creation of electronic documents with electronic signatures in various institutions, organizations, governments and private sector[68].

[67] See Section 10(1),Ibid

[68] Mambi, Adam J, 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.

Zanzibar as other countries have been seeing the rapid development of information technology in hardware and software. The current offence like cybercrime especially in e-commerce will require prove using electronic evidence. Zanzibar in evidence decree are not mention any electronic evidence but give the right for judiciary to refer from other countries for decision any case include cases related to cybercrime:

> *When the court has to form an opinion as to a law of any country, any statement of such law contained in a book purporting to be printed or published under the authority of the Government of such country and to contain any such law, and any report of a ruling of the courts of such country contained in a book purporting to be a report of such rulings, is relevant.*[69]

4.3.10 The Children Act 2011

The Revolutionary Government of Zanzibar passes the Children Act in March 2011. The Acts cover the fundamental rights of children and focus on Child protection strategies in a range of abuse, violence and exploitation of children. These laws for children effectively domesticate the UN Convention on the Rights of the Child which was ratified by Tanzania in 1991. They address such fundamental issues as non-discrimination, the right to a name and nationality, the rights and duties of parents, the right to opinion and the right to protection from torture and degrading treatment[70].

In part IV of the Act state on Care and Protection of a Child:

[69]The Anti-Money Laundering and Proceeds of Crime Act No. 10,2009, S.38
[70]http://www.unicef.org/tanzania/6908_10614.html, finding March ,17th 2014

(*f) a child who is engaged in commercial sex work or has been subjected to any form of sexual exploitation*[71].

The statement "*any form of sexual exploitation*" in section 19(2) above include criminal which performed to child through internet.

4.3.11 The Electronic and Postal Communication Act (EPOCA) of 2010

Tanzania Communication Regulatory Authority (TCRA) is the regulator responsible for communication and broadcasting in Tanzania. On other hand broadcasting sector in Zanzibar is regulated by the Zanzibar Commission (ZBC) and leaving the communication sector in Zanzibar to be regulated by TCRA. But on the issue of Sim card registration was passed in both part of the union in order to stop any kind of crime which have been commits through Mobile Phone. In EPOCA of 2010 under the section 131, stipulates that it is a criminal offence for any person who knowingly uses or causes to be used an unregistered SIM and shall be liable on conviction to a fine of five hundred thousand Tanzanian shilling or imprisonment for a term three months[72].

For now, an Act to make provisions for the enactment of electronic and postal communications law with a view to keeping well-informed with developments in the electronic communications industry ready, The Act has Objectives to provide for a comprehensive regulatory regime for electronic communications service providers and postal communications service providers, to establish the Central Equipment Identification Register for registration of detachable SIM card and built-in SIM card

[71] The Children Act 2011,S.19(2)
[72]TCRA, Public Notice 30th May 2013

mobile phones to provide for duties of electronic communications and postal licensees, agents and customers, content regulation, issuance of postal communication licences and to regulate competitions and practices, to provide for offences relating to electronic communications and postal communications and to provide for transitional provisions, consequential amendments and other related matters[73]. This exercises of SimCard Registration leading by The Tanzania Communication Regulatory Authority (TCRA)[74]. The objectives of this law is to protect customer from misuse of their phone in their communication.The registration is important because company provides Mobile Money and allow transaction through the customer mobile Phone .The registration of SIM Card help to stop crime.The Mobile Phone Services Provider not allow any mobile SimCard to operate without the registration either to services Provider or Agent of the Company. Also registering the Sims customers help to identify those use their SimCard for crime activities, increase a security due to mobile banking and mobile money transfer like M-Pesa, Easy Pesa and Airtel Money.

4.3.12 Banking and Financial Institution Act No 5 of 2006

This Act apply to both parts of union Tanzania Mainland and Zanzibar. Because the regulation of Banks and Financial system is control under BOT which is a union matter. The Act is provide a comprehensive regulation of banks and financial institutions. It provide a regulation and supervision of activities of savings and credit co-operative societies and schemes with a view to maintaining the stability,

[73]See Tanzania Communications Services (Licensing) Regulations 2005, enacted under Electronic and Postal Communication Act No 3 of 2010.
[74]TCRA Act No. 12 of 2003

safety and soundness of the financial system aimed at reduction of risk of loss to depositors; to provide for repeal of the Banking and Financial Institutions Act, (Cap.342) and to provide for other related matters. In PART VI give state the power to make Supervision, Coordination and Control:

> *(1)Notwithstanding any provision to the contrary contained in any written law, the Bank shall have power to access to any oral and documented information, including information in computers, books, minutes, accounts, cash, securities, documents, vouchers as well as any other things in the possession or custody or under the control of a bank or financial institution or its affiliate, which relate to the business of such bank or financial institution*[75].

The power to conduct inspections of banks and financial Institutions is allowed to the Bank to access customer information. This right will help to prevent cybercrime since the law give the permission to access information including in computer and related business.

4.4 Challenge of Laws to Combat Cybercrime in Zanzibar

4.4.1 The Challenge of Zanzibar Contract Decree

In cyberspace electronic contract is compulsory especial in electronic Commerce and other online business like Online Banking.The law of contract usually determines the relationship between Supplier and customers in which there should be a contract between in respect of their rights and duties for each one. The relationship between

[75]Banking and Financial Institution Act No 5 of 2006, S.31

Supplier and customer is a contractual relation, which is the contract by conduct which is principal and agent depending upon the nature of the business. Therefore, the electronic contract is important to be accepted in law to protect society from the cybercrime. It important to note that traditional contract made is not the same with that of the electronic payment. It seems that the Zanzibarcontact decreenot accept the parties to enter into electronic contract. Because there is no provisions which identify the recognition of electronic contact.This give the opportunities to cybercrime to perform their illegal action.

In Part II[76]provides that,

> "*Nothing herein after contained shall affect any law in force in Zanzibar, and not hereby express repealed, by which any contract is required to be made in writing or in the presence of witness, or any law relating the registration of documents."*[77]

Also it has witnessed that, in order a contract to be accepted must be written and to be signed by the parties[78], It provides that An agreement made without consideration is void, unless:[79]

> *(a)It is expressed in writing and registered under the law for the time being in force for the registration of documents and is made on account of natural love and affection between parties standing in a near relation to each other or unless;*

[76]Zanzibar Law of Contract Decree, Chapter 149 of 1917
[77]Section 10 (2)
[78]See section 25(1)(a)(b)(c) ibid
[79] section 25(1)(a-c)

(b)It is a promise to compensate, wholly or in part , a person who has already voluntarily done something for the promise, or something which the promise was legally compellable to do or unless; and

(c)It is a promise made in writing and signed by the person to be charged therewith or by his agent generally or specially authorized in that behalf, to pay wholly or in part a depth of which the creditor might have enforced payment but for the law for the limitation of suits.[80]

Under thisanalysis we can say that, the Zanzibar Contract Decree is not including the use of electronic Contractand does not recognize the digital signature[81].This is very risk for Zanzibarsociety to enter into electronic business because criminals can take the chance to perform their crimes especial in electronic transaction through banks and electronic commercethat can cause to loss their money, and the laws is not sufficient to deals with the types of electronics practices[82].

4.4.2 Challenges of Zanzibar Criminal Procedure Act

Until now the Acts identifies all committed traditional crimes and not crimes related with computer, internet and network systems. But even though to somehow in some provisions the Act has provided to some extent the procedures in prosecuting and investigation of some issues related with computer and electronic transactions. Although Mobile Banking and email banking operate in Zanzibar but the laws, it just accommodates the ordinary financial transaction even though it transaction is

[80]ibid
[81]See Trust Bank Ltd V. Le Marsh Enterprises Ltd and others. H.C (Com. Div) at DSM CC No. 4 of 2000 (unreported)
[82] See Adam .J. Mambi, *I CT Law Book, A Source Book for information & Communication Technologies and cyber law*MkukinaNyota Publisher, Dare es salaam, 2010, page 127 .

associated with computer data but the provision seems to be not clear so far. For example, investigation involve online transaction crime section 134 provides[83]:

> *whenever the Director of Public Prosecutions considers it necessary that a bank account or accounts or any other financial transaction should be investigated in connection with any crime alleged to have been committed the Director of Public Prosecutions may by order in writing authorize a police officer of a rank not below assistant inspector or any other person to investigate the said account or the said financial transaction and may order the bank to temporarily suspend the operation of such account pending such investigation.*[84]

Therefore, the section is contradicting with the sections under the Evidence Decree since that the Evidence Decree does not show the admissibility of electronic evidence as shown in the Criminal Procedure.

For example a case reported at Zanzibar Town Regional Police Station (Madema) on theft by using Visa Card:[85]

4.4.3 Case Law

ASP Abrahman V. Ahmed Sultan and Walas Lawrence [2014] MAD/RB/ 656

The case is under investigation at Madema Police Station. Also we can observe that, the court has been settled the powers for somehow to declare evidence through electronic media in some cases. On the other hand, it shows the admissibility of electronic evidence, the provision is not strong to cover the situation and in

[83]The Criminal Procedure Act No.7, 2004
[84]Ibid
[85]MAD/RB/ 656

somehow it contradicts with Evidence Decree[86] which does not provide that there could be a possibility of evidence to be printed if it has originated in electronic media. So that cybercrime can take advantage to perform their crime due to the weakness and contradiction of the law.

In Section 269 of the Criminal Procedure Act provides:

The court may in appropriate case allow evidence to be adduced by witness through electronic media. The court may allow witness to give evidence through electronic media only in the following circumstance: where identity of a witness may be ascertained and where examination may be conducted without hindrance.[87]

So, in this respect these laws are subject to major amendment so as to be consistent on how the evidence in electronic form can be adduced and to be admitted in the court as well as to reflect the online transaction practices in electronic activities. Therefore, neither the Criminal Procedure Act[88] nor the Evidence Decree directly provide for the admissibility of the electronic evidence or electronic documents even though the Criminal Procedure Act[89] has granted the power to the court to order search, seizure of computer data and equipment. Also the production of data, where the Director of Public Prosecution may order the production by a person in control of a computer system as per section 138 (a) and (b) have the effect that` electronic evidence is admissible.

---

[86]Ibid
[87] Ibid.
[88] Sections 132 and section 142 of Criminal Procedure Act, Act no. 7 of 2004.
[89]Section 135(1),(a), (b) and (2),(a),(b) and section 138 (a), (b) of Criminal Procedure Act, Act no.7,2004.

Section 135(1) provides that:

> *If a magistrate is satisfied in the basis of information on oath that there are reasonable grounds to suspect that there may be in a place a thing or computer data: (a) that may be material as evidence in proving an offence; or (b) that has been acquired by a person as a result of an offence; the magistrate may issue a warrant authorizing a police or any authorized person to enter the place to search the thing or computer data. (2) In this section "thing" includes: (a) computer system or part of a computer system; and (b) a computer data storage medium.*[90]

4.4.4 Zanzibar Penal Act No.6 of 2004

Panel Act No.6 of 2004[91] provides for the offences connected with computers as seen above but on the other side it seems to controvert with the Evidence Decree[92] which does not show any the procedures on how to verify the evidence electronically or related with computers. Another Challenge, the Act only provides the numbers of offences committed in ordinary theft but does not cover other offences committed electronically theft like those who stolen sensitive data through internet, computer and network system. This Act defines provides for the definition of theft as:

> *A person who fraudulently and without claim of right takes anything capable of being stolen, or fraudulently converts to the use of any person other than the general or special owner thereof anything capable of being stolen, is said to steal that thing.*[93]

---

[90] Ibid
[91] Section 372 and section 381
[92] The Zanzibar Evidence Decree Cap 5 of 1917
[93] See section267(1),Ibid

The definition includes the numbers of theft but on the other way does not say about theft committed electronically and how it could be proved under the evidence Decree.

4.4.5 The Zanzibar Anti-Corruption and Economic Crimes Act, 2012

For the digital World, sometime it difficult to separate the impact economic crime and cybercrime. Cybercrime cost the world economy billion of dollar every year, due to the damage of business by hacking and theft of intellectual property, business and Government information. The Revolutionary Government of Zanzibar established an Act[94] for the function to prevent corruption and economic crime and with others matter connected therewith but the law did not mention a cybercrime to be one among the substance which can be commit as an offence of economic crime. The Actstate only on money Laundering

> *Any person who engages in or does an act constituting an offence of money laundering under the Anti-Money Laundering Act No. 10 of 2009 commits an offence of economic crime under this Act.*[95]

Also Act is state on drug trafficking but did not mention any offence performed by means of trafficking related to through internet and computer network.

> *Any person who by any unlawfully means imports, exports, manufacture, buy, sale, gives, supplies, stores, administers, convey delivery or distributes, by any person of narcotic drug or psychotropic*

[94]The Zanzibar Anti-Corruption and Economic Crimes Act, 2012
[95]See Section 49, ibid

substance or makes offer of narcotic drug or psychotropic substance commits an offence of economic crime under this Act.[96]

Zanzibar need to make amendment on this Act to combat cybercrime because has a serious implication for economic. This is a very challenge to Zanzibar laws because cybercrime, economic crime and corruption in general are related things.

4.4.6 Zanzibar Evidence Decree

The Zanzibar common law legal system related to business and civil matter. Its evidence was made to suit physical on the use of traditional (paper based) method. The digital world makes the situation of business to be different because of the fact that parties are not physical meet or spoken during the agreement. It possible to face problems on the acceptability and weight of this kind of evidence because the documents will be look upon is generated by computer which in most case taken as secondary and not primary evidence.

Most our statutes about evidence support the requirement of written original document, for the best evidence rule require only original document can be admissible in our court of law.

In evidence decree state that

When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or a connected series of letters or papers, evidence shall be given of so much and no more of the

[96]Ibid, s.50

statement, conversation, document, book or series of letters or papers as the court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made[97].

The sections above, which show the statement made under special circumstances to be considered relevant when adducing before a court to be evidence, do not include the statement made in electronic form which is printed in a paper. The sections only accommodate documentary evidence. Due to the development of digital technology, computers and network system affect the use, scope and admissibility of electronic evidence. So, there is no provision of law which provides for electronic evidence or its presumption.

4.4 Field Analysis

In this part, provides the response to the facts obtainable during the interview of the study. Information from the time of discussion of the study have been taken as the basis of explanation and investigation of the study. Effort was made to relate the validity of the legal documents and responses officer from legal and ICT institutions. Practical situation was done to see in general the reality of cybercrime issue and Zanzibar legislation.

4.4.1 Relevance of the Laws to Cybercrime

During the interview one among the question raised to officers was on relevance of the Zanzibar laws to cybercrime. Direct the answer respond that the laws governing

[97]Ibid ,S.39

cybercrime were legislatedearlierthan the development of Information Technology in Zanzibar. Theysaid that not relevant to meet the requirement of the cyberspace and suggested the amendment of the laws governing cybercrime.

Althoughamendment was done to the laws of Zanzibar but not enough to prevent a cybercrime.This is because most of the laws are out of date. For Example the Evidence Decree it is established since 1967, it was copied from Indian Evidence Act. The Act it has been amended in order to meet demand of prosecution in Zanzibar but until now no one of improving solve the challenges of electronicEvidence. There is a need of reviewing the laws in order to counter problems concerning cyberspace in Zanzibar.

4.4.2 Awareness on Cybercrime

Another question was upon awareness of Zanzibar society about cybercrime. The both respond was that most of the people in Zanzibar are unaware with the cybercrime and cybercrime law. While on the answers concerning additional question about the cybercrime cases reported, they said, most of cases are not reported at police or other legal office. Also is the fact that most of those reported cases are not reach the stage of hearing at court due to that the lack of evidence and proper way for investigation. According to the Police Officer most of cases reported is mobile abusive language or SMS. For example

A case reported at Madema Police Station which is under investigation:

Khadija Hamid V unknown MAD/RB/2529 2013

For the question regarding on which existence of laws used to conduct those cases, the answers that they relate case with traditional laws and most of cases are in the clear and in their explanations it was found that the evidence given is not relevant to the cases concerning cybercrime.

4.4.3 Shortage of well Qualified Professionals of ICT in Cybercrime

There is a scarcity of well skilled professionals of ICT in Zanzibar. However, there is a number of ICT experts working in differentinstitution spread around the country. Although, there obtainable ICT experts are underutilized in comparison with their potentials. There are also no entrenched ICT professional outlines and lack of a consistent process of evaluation for certification of different ICT courses offered by various training centres. Moreover there is no documented plans or strategies for developing ICT literacy skills of the existing manpower in both public and private sectors.[98]

4.4.4 Lack of Support to Collect cybercrime Evidence from other Stakeholders

Effective argue against cybercrime will be successful only if there is strong law enforcement agencies and involvement of all stakeholder in Zanzibar and around the world. The services Provider, civil society, ICT technician, lawyers, business and Government are very important parts to prevent cybercrime. But one among saddest issue arise during the interview is Police officer lack support from other Mobile company especially TIGO Mobile Company in Zanzibar to declare details of the suspected person. TIGO did to hide customer information because there is no law

[98]Zanzibar ICT Policy, First Edition, June 2013, pg 6

bind them. For example Case reported at MademaPolice Station; Asha Khamis Ali v unknown MAD/RB/216 15.01.2013

The case of abusive words through mobile phone, the unknown person was used TIGO Mobile SimCard. The case was closed TIGO collect nearly 16% of customer in Zanzibar and make to be a second company after ZANTEL which collect more than 80% of customer and rest of customer use others company called Airtel and Vodacom. But Police officer said that ZANTEL it is fast to declare information once is needed.

4.5 Strategies for Zanzibar to Initiate Cybercrime Law

4.5.1 Implementation of ICT Policies

The Revolutionary Government of Zanzibar has recognized the fundamental importance of ICT for stimulation of national development, in particular, modernization and globalization of the economy and creating the conditions for the fullest participation by all sections of the population.

4.5.1.1 Zanzibar ICT Policy

The Government of Zanzibarintroduce a very comprehensive ICT policy. The policy will guide and mention the development of ICT in Zanzibar,convenience and its operation on a national measure to meet the challenges of the Digital information andplace the foundation for the development of Zanzibar ICT strategic Plan. The Revolutionary Government of Zanzibar has recognized the fundamental importance of ICT for stimulation of national development, in particular, modernization and globalization of the economy and creating the conditions for the fullest participation

by all sections of the population. Zanzibar achieved notable progress in deploying ICT; the private sector has actively contribute to these achievements by investing inter-alia support facilities, training centres and sales outlets. These efforts have enabled Government departments, institutions of learning, NGOs as well other entrepreneurs; to acquire ICT solutions that address their individual problems.[99]

4.5.1.2 E-Government Policy

The Revolutionary Government of Zanzibar (RGoZ) is in the verge of introducing e-government system with the aim of improving service delivery, in line with Zanzibar strategy for growth and Reduction of Poverty (ZSGRP II) for attaining the Zanzibar Vision 2020 and Millennium Development Goals (MDGs). E-Government refers to the use of Information and Communications Technologies (ICT) to improve efficiency, effectiveness, transparency and accountability of government on service delivery. E-Government can be seen simply as connecting citizens, businesses, and employees to government services online, but in its broadest sense it refers to the technology-enabled transformation of government services.[100]

4.5.2 Development of ICT Human Resource

The Revolutionary Government of Zanzibar established and implementation new scheme of services for ICT professionals servants and dedicate to recruit her expertise oversee public in order to get more skills. Above all, more colleges and universities are motivated to provide various training programs in Computing

[99]Zanzibar ICT Policy, First Edition , June 2013,pg3
[100]Zanzibar e-Government Policy, June 2012,pg2

Studies and Telecommunication. The course provides are directed to be high level ranging from certificate to Postgraduate. The Ministry of Education was responsible to prepared curriculum that integrate ICT for mandatory education.

4.5.3 To establish ICT Infrastructure

In Zanzibar, there is tremendous growth in ICT infrastructure. The Revolutionary Government of Zanzibar deployed fibre optical cable across both islands of Unguja and Pemba and capacious microwave link connecting the Islands. There are two fibre optic terminals connecting Zanzibar and Tanzania Mainland forming a ring that provides resilience to deployed network. Furthermore,Telecommunications companies launched 3G and 4G network providing fast access of ICT services such as Internet to Zanzibar Community.[101]

4.5.4 To Amend a Comprehensive Laws to Reflect on Cyberspace

Most of interviewee replied that the laws are not relevant to cybercrime. And they mention that there are different laws in prosecutions that are to be amended so as to reflect the prevention of cybercrime in Zanzibar. They was of the outlook that the trial is placed in difficulties when there is a case concerning cyberspace. Participants in their discussion on regulation to the fighting cybercrime, noting that it is important to develop a legal frame work as well as new technology and organization mechanism to combat cybercrime.

4.5.5 To established Police Cybercrime Division

In Tanzania Police is a union matter. It work both side of the union. The relationship

[101]Zanzibar ICT Policy, First edition, 2013, pg6

between police and cybercrime is for looking how police can arrest those who commit crime by using computer and related technology. The Capacity of the Police Force in Tanzania to combat property related crimes and new emerging crimes such as human trafficking and cybercrimes is also very low[102]. This because of lack of technology and intelligent technician. Now Tanzania Police Force try to introduce strategies to prevent cybercrime gradually. They initiate a Cybercrime Division for cybercrime investigations and evidence collection. This is very important every nation is responsible for security of their citizens especially protection and combating any type criminal. This will achieve by established strong professional institutions and investing good equipment's and technicians.

[102]Tanzania Human Right Report 2012

CHAPTER FIVE

5.0 CONCLUSION AND ECOMMENDATION

5.1 Introduction

The development of ICT has introduced new method of life. The development of technology change rapidly mode of communication, and daily human activities. To keep up coordination of society in this cyber spaces there is a need for Zanzibar to introduce a legal system to establish a Cyber law. Because a Cyber law are the basic laws and effective on every aspect of the cyber society such as Business, Information Delivery, Governance, Education and Intellectual property.

5.2 Conclusion

This study, based on the critical analysis on how Zanzibar legal system is successful to combat cybercrime. In which it has been found that the laws are outdated and do not reflect direct to prevent a cyber-crisis.For example, the penal laws and criminal procedure laws do not recognize the cybercrimes although include crime offence like banking crimes but did not mention crime conducted through electronic means.

The conclusions of this study show that, a number of laws governing crime in Zanzibar are out dated since there new type crime commit through Computer and related activities. The laws are not relevant to Digital World. It consequence is that, most of the cases are reported found isnot guilty due to the fact that the evidence given does not reflect on electronic Technology.And the rules applied in citing evidence are almost based on local means which originated from traditional method like paper document.

Moreover, from the above analysis and responds during the study it is obvious to say that, Zanzibar legal framework is not adequate to regulate cybercrime. As well as the public is unaware of the modern threats posed in cyberspace. The amendment of Zanzibarlaws like the Evidence Decree, the Criminal Procedure Act and other comprehensive lawsis compulsory in order to fight well for cybercrime war. Therefore the study experienced that there is a lack of support within the stakeholders at a time of case investigation. The cooperation among participants in war is very important to combat cybercrimes. The Revolution Government of Zanzibar must to keep more effort to establish a law which can bind both stakeholder who not deliver information during the investigation of cases.

The policy and legal strategic can bring the Zanzibar governments and responsible institutions to set law and regulation to punish those deals with this unfair business. Legal actions play a major key role to prevent and combating of cybercrime. In order to reduce the cybercrime problem, law is must be dynamic tool that can enables the states to respond to any kind of criminal, new cybercrime challenges and maintain security. For best result national laws and international laws both must covers laws that are related to cybercrime.

5.3 Recommendation

5.3.1 Establishment of Cybercrime Laws

The Government of Zanzibar is necessary to established new laws which is specific for cybercrime. The framework must be effective for strategies on cybercrime legislation and enforcement. It is important for framework to relate with the Budapest Convention and to work of the Council of Europe Convention of

cybercrime guidelines as a reference materials because it the best Framework of International Cooperation to prevent cybercrime.

5.3.2 Amendment of Zanzibar Laws

Zanzibar Laws should be amended to include cybercrime provisions. Because the laws were enacted before people of Zanzibar experiences digital technology in high level. The amendment of laws to include provisions on admissibility of electronic evidence, penal Act and Criminal Procedure so as to accept the new technology in order to recognize the offence committed through electronic media. The amendment of procedural laws should include electronic technology and/or intangible evidence needs to combat cybercrime. Because it is possible for criminals to practices new forms of cybercrime will frequently develop with changing technology. Thus the Laws must to respond to these rapid changes.

5.3.3 Improve Technical Assistance

The Government Zanzibar should invest capacity building for his expertise, magistrates, prosecutors, investigators and judges to the collection and analysis of electronic evidence. Also to support the governing authorities such as equipment and skills for the purpose of regulating any kind of cybercrime.

5.3.4 To initiate Trans Border Cooperation

Law enforcement agencies in Zanzibar should develop trans-border cooperation to help quicker responses to cybercrime through the sharing of information, experience and good practices. Also should increase collaboration with East African Countries to promote involvement to encounter the needs of African jurisdictive and in the

concern of cybercrime legislation. Therefore is important to relate with international conventions through the Government of Tanzania for legal assistance guidelines.

5.3.5 Performing ICT policy to Meet the Requirement to Protect Cybercrime

The ICT policy should adopt security and usage of ICT to improve quality, accessibility, affordability and provision of services to the public. Also the Policy should state that the Government must review existing laws and regulations in order to favourable the growth of ICT industry and International Conventions to prevent cybercrime.

5.3.6 Awareness to the Zanzibar Society

Peoples in Zanzibar should be modernised and be given awareness on cyberspace and the threats posed to it. The basic education should be introduce from primary education in order to litigate any troubles can be occurred due to new technology. Awareness can help them to avoid any risk in their communication through the internet, bank systems, mobile communication and other activities with related to digital technology. Also awareness must be introduce to legal officer, Courts, Police officer and ICT technician because they responsible to collect evidence everyone in his/her part when a matter arise and avoid cheating in adducing evidence.

5.3.7 Established Forensic Laboratory

This laboratory will help to the legal evidence which found in computer and other related digital technology. The computer forensics is to inspect digital media for the aim of analysing, preserving, identifying, recovering and presenting facts and

opinion concern to digital information. This is very important for cybercrime war because investigation through computer forensic are acceptable for most of cases of cybercrime.

REFERENCES

Adam .J. Mambi, I CT Law Book, A Source Book for information & Communication Technologies and cyber law MkukinaNyota Publisher, Dare es salaam, 2010

Alkaab, Ali, Combating Computer Crime: An international and Perspective, Oct 2010, Queensland University of Technology, http://eprints.qut.edu.au/43400/1/Ali_Alkaabi_Thesis.pdf (accessed 04th July)

Banking and Financial Institution Act No 5 of 2006

Carter, E, *Examining Cybercrime: Its Forms and Its Perpetrators*, 2002, NUIA, Kiev

Copyright Act No.14 of 20032014).

Donald KisiluKombo and Delno L.A Tromp, Proposal and Thesis writing, https://www.fiu.go.tz/TanzaniaNationalAML-CFTstrategy.pdf, (accessed 9th July 2014).

Electronic and Postal Communication Act No 3 of 2010.

G8 Deauville Declaration: INTERNET

General Assembly resolution 65/230

http://aspireip.com/cyber-crimes-space-and-so-forth-a-concept-of-cyber-laws/,(accessed 01st July 2014)

http://conventions.coe.int/Treaty/EN/Reports/html/185.htm, (accessed 17th July 2014).

http://conventions.coe.int/Treaty/EN/Summaries/Html/201.htm, (accessed 08th July

2014).

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, (accessed 02nd July 2014).

http://definitions.uslegal.com/c/cyber-law, (accessed 2nd July 2014).

http://law.jrank.org/pages/11992/Cyber-Crime-Intellectual-property-theft.html,(accessed 01st July 2014)

http://studentresearch.ucsd.edu/_files/assessment/Assessment-Methods.pdf, (accessed 05th July 2014).

http://www.aaregistry.org/historic_events/view/zanzibar-gains-independence-britain, (accessed 23rd July 2014).

http://www.bbc.co.uk/schools/gcsebitesize/ict/legal/2copyrightrev1.shtml,(accessed 03rd July 2014).

http://www.brighthub.com/internet/security-privacy/articles/3435.aspx,(accessed 03rd July 2014)

http://www.cybercrimelaw.net/International_organizations.html, (accessed 11th July 2014).

http://www.doc.gold.ac.uk/~mas01rk/Teaching/CIS110/notes/Computer-misuse.html, (accessed 05th July 2014).

http://www.drcath.net/toolkit/document.html, (accessed 28th June 2014).

http://www.g8.utoronto.ca/summit/2011deauville/2011-internet-en.html, (accessed 15th July 2014).

http://www.law.cornell.edu/wex/computer_and_internet_fraud, (accessed 12th July 2014).

http://www.melissavirus.com, (accessed 2nd July 2014).

http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective, (accessed 20th July 2014).

http://www.nature.com/bdj/journal/v204/n6/full/bdj.2008.192.html, (accessed 18th July 2014).

http://www.oecd.org/internet/ieconomy/15582260.pdf, (accessed 07th July 2014).

http://www.pandys.org/articles/sexualabusegrooming.html,(accessed 01st July 2014)

http://www.peacepalacelibrary.nl/2013/10/protecting-children-from-cybercrime-online-child-grooming/,(accessed 07th July 2014).

http://www.techterms.com/definition/cybercrime, (accessed 02nd July 2014).

http://www.unicef.org/tanzania/6908_10614.html, (accessed July, 17th 2014).

http://www.websitedefender.com/what-is-malware/, (accessed 06th July 2014).

https://www.europol.europa.eu/ec3old, (accessed 25th June 2014).

https://www.europol.europa.eu/sites/default/files/publications/ec3_first_year_report.pdf, (accessed 02th July 2014).

https://www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf, (accessed 17th July 2014).

https://www.gov.uk/data-protection/the-data-protection-act, (accessed 14th July 2014).

Ian J. Lloyd, Information Technology Law, 6th Edition, 2011, Oxford University Press, New York

Mambi, Adam J, 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.

Mollel, Andrew L. &Lukumay, Zakayo N., Electronic Transactions and The Law of Evidence in Tanzania, 2007, IUC, Tanzania.

Nyamaka, Daudi, Electronic Contracts in Tanzania: An Appraisal of the Legal Framework,2011,SAUT, Tanzania

OECD Guidelines for the Security of Information Systems and Networks TOWARDS A CULTURE OF SECURITY.

Ozeren, Suleyman, Global response to cyber terrorism and cybercrime: A matrix for International cooperation and vulnerability assessment,digital.library.unt.edu/ark:/67531/metadc4847/m2/.../dissertation.pdf (accesses 28th June 2014).

Patrick Mwaita And Maureen Owor (Accp),Workshop Report on Effective Cybercrime Legislation in Eastern Africa Dar es Salaam, Tanzania, 22-24 August 2013.

Prevention of Terrorism Act (URT),2002

Public Services Acts No.2 of 2011.

resolution 67/184, CCPCJ

Sheakh, T, Cyber Law: Provision and Anticipation, 2012, Vol. 53 No.7.

Tanzania Communications Services (Licensing) Regulations 2005

Tanzania Human Right Report 2012

TCRA Act No. 12 of 2003

The African Centre for Cyber law and Cybercrime Prevention (ACCP)

The Anti-Money Laundering and Proceeds of Crime Act No. 10,2009

The Children Act 2011,

The Constitution of United Republic of Tanzania, 1977

The Council of Europe Convention on Cybercrime.

The Employment Act No. 11, 2005.

The of Criminal Procedure Act, Act no.7,2004

The UK Computer Misuse Act

The Zanzibar Anti-Corruption and Economic Crimes Act, 2012

The Zanzibar Constitution 1984

URT, Strategy for Anti-Money Laundering and Combating Terrorist Financing, July 2010 June 2013.

Vatis, Michael , The Council of Europe Convention on Cybercrime, https://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf(accessed 03rd July 2014)

Workshop report on effective cybercrime legislation in eastern Africa, Dar es salaam, Tanzania, 22-24 august 2013 Written by Patrick Mwaita and Maureen Owor (ACCP)

www.computerevidence.co.uk/Cases/CMA.htm, (accessed 28th June 2014).

www.univd.edu.ua/_projects/ezloch_kor/docs/eng/37.doc, (accessed 11th July 2014).

Zanzibar e-Government Policy, June 2012

Zanzibar Evidence Decree Cap 5 of 1917

Zanzibar ICT Policy, First edition, 2013

Zanzibar Law of Contract Decree

Zanzibar Penal Act No.6 of 2004.