ELIMINATION OF CYBERCRIMES IN TANZANIA: LAW AND PRACTICE

ANIPHA ABASS MWINGIRA

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF THE MASTER OF LAW IN INFORMATION TECHNOLOGY AND TELECOMMUNICATION (LLM IT & T) OF THE OPEN UNIVERSITY OF TANZANIA

2013

CERTIFICATION

The undersigned do certify to have read and hereby recommend for acceptance by The Open University of Tanzania a Dissertation entitled: **Elimination of Cybercrimes in Tanzania: Law and Practice**; in partial fulfillment of the requirement for the Masters Degree in Information Technology and Telecommunication Law.

……

Prof. Ian. J. Lloyd

(Supervisor)

……..

Date

COPYRIGHT

DECLARATION

I Mwingira, Anipha Abass, to the best of my knowledge and belief, do hereby declare that, this Dissertation is a product of my own efforts. It has neither been duplicated nor submitted to any other university for a similar study to be undertaken.

……

Signature

……

Date

DEDICATION

This dissertation is dedicated to my parents.

ACKNOWLEDGEMENT

This Dissertation would not be a success had it not been the encouragement from my Supervisor Professor Ian Lloyd, my course coordinator Dr. Susan Kolimba and Gervas Yeyeye, of the Open University of Tanzania to research on this topic. I am much indebted for their guidance and advice throughout the preparation of this Dissertation.

I am also much indebted to Dr. Zakayo Lukumay for moral support and going through this Dissertation as a second eye. At the eleventh hour he has been ready to go through my script and putting his valuable contribution. My colleagues at my working place Kinondoni Primary court for understanding me and supporting me to pursue this research. I am much indebted to them.

It is not easy to name each one who has aided me in the preparation of this Dissertation. I wish to thank all those who are not mentioned but have rendered their support during the preparations of this theoretical framework of the study envisaged.

While I appreciate the assistance extended to me by all, any failure or gaps in this theoretical framework remains solely on me.

ABSTRACT

The focus of this research was to examine how the existing penal laws can be used to combat cyber crimes in Tanzania. It sought to examine the efficacy of the legal framework in combating cybercrimes in Tanzania. In the course of conducting this research, various methods were used. The main ones were library research and field work. Various individuals were interviewed as reflected in the text. The aim was to get data, cases, and views in relation to the subject of this study. It was observed that today's society has been dependent on computer and computer networks – the Internet. In other words, nothing so far can be done without computers. Criminals on the other hand have made use of the technology to perpetrate their ill motives. In other words, dependence upon technology has made electronic offences to increase. The analysis made in so far as the Penal Code of Tanzania is concerned is that it is not keeping pace with technology. Its provisions as discussed show that they are paper and physically based. It is argued that, endeavor of law making machinery of the nation should be in accordance with mile compared to the fraudsters, to keep the crimes lowest. Hence, it should be the persistent efforts of rulers and law makers to ensure that governing laws of technology contains every aspect and issues of cyber crime and further grow in continuous and healthy manner to keep constant vigil and check over the related crimes. It is for this reason that the Penal Code should be amended to provide for criminal activities conducted using computers and computer networks. The offences that should be introduced in the Penal Code are hacking, illegal access to computers and computer networks, fraud committed using computers and computer networks, money laundering and related crimes, identity theft, and many others in this respect.

TABLE OF CONTENT

LIST OF CASES

LIST OF LEGISLATION

International Instruments

Berne Convention, the copyright and Neighboring Right Act No. 7 1999.

United Kingdom Computer Misuse Act 1990.

Data Protection Act 1984

The Reserve Bank of India Report on Internet Banking 2001.

India Information Technology Act No. 21 of 2010

The German Data Protection Act 1970

The Malaysia Computer Crimes Act 1997.

United Stated Computer Fraud and Abuse Act.

The Indian Penal Code.

The European union convention on Cybercrimes.

Local Legislation

The Tanzania Penal Code CAP 16 (R.E 2002)

Electronic and Postal Communications Act (EPOCA) of 2010.

Anti Money Laundering Act 2006.

National Information Communication Technology Policy 2003.

Money Laundering Act 2009.

ABBREVIATIONS

TRA	:	Tanzania Revenue Authority
EPOCA	:	Electronic and Postal Communications Act
TCRA	:	Tanzania Communications Regulatory Authority.
IT	:	Information Technology
ICT	:	Information Communications Technology
ITA	:	Information Technology Act
NIGF	:	National Internet Governance Forum.
DPP	:	Director of Public Prosecutions
DR	:	Doctor
E-money	:	Electronic Money
ATM	:	Automated Teller Machines
E-banking	:	Electronic Banking
SMS	:	Short Message Service
MMS	:	Multi Media Service
E-commerce	:	Electronic commerce
IGF	:	Internet Governance Forum
UK	:	United Kingdom
US	:	United States
USA	:	United States of Africa
PPF	:	Public Pension Fund
E-books	:	Electronic Books
E-mail	:	Electronic mail
Etc	:	Et cetera

www	:	World Wide Web
PCI	:	Payment Card Industry
PIN	:	Personal Identification Numbers
ID	:	Identity Card
FSA	:	Financial services Authority
R	:	Republic
V	:	Versus
SWIFT	:	Society Worldwide Interbank Financial Telecommunications
NMB	:	National Microfinance Bank
TUCTA	:	Trade Union Congress of Tanzania
NGO	:	Non Governmental Organization
US	:	United States Dollar
SADC	:	Southern Africa Development Community
NBC	:	National Bank of Commerce.
No	:	Number
ALL ER	:	All England Report
NCRB	:	National Crime Records Bureau
ITAA	:	Information Technology Act Amendment.
CD	:	Compact Disc.

CHAPTER ONE

1.0 INTRODUCTION AND BACKGROUND

1.1 Introduction

Cybercrimes can be defined as offences that are committed against individuals or groups of individuals through electronic means and telecommunication networks like internet chart rooms, emails, mobile phones by way of text messages.[1] Like any other crimes, computer crimes tend to pose dangers to national security and can as well be a threat to financial security if not well addressed.[2]

Cyber crimes are growing exponentially in big cities of Tanzania where telecommunications via electronic means is widely used. These cities are like Arusha, Dar es Salaam and Mwanza where there has been evidence of occurrence of incidents of cyber crimes. This has presented formidable threat to our society particularly on young ones who may be obsessed by offences like cyber pornography.

Recently, the governments of Tanzania have taken measures to ensure that all sim cards are registered for the purpose of preventing abuse of mobile phone usages. By doing that, it was hoped that cyber crime may decrease. There is currently a move targeting cyber cafés operators who will soon be required to register all their customers and this is a proposal made by the police Department. The aim behind such move is to arrest all perpetrators of cyber crimes through mobile phones and the internet.

---

[1] Cited at http:/allafrica.com/stones/201206270137.html?-aa-sauce=useful-column
[2] Ibid.

In Arusha, for example, one man was arrested at a certain local bar on allegation that he had committed a cybercrime. Prior to his arrest, there were allegations that the person had a barbershop and one of the services he offered was charging phones. He was tempted to use his clients' money to access their M-Pesa accounts and transfer money to himself. It has been reported that over five hundreds (500) Tanzanians have been apprehended by the cybercrimes unit between 2011 and 2012 over cyber crimes allegations.[3]

The deputy Home Affairs Minister of the country Honorable Penaira Amesilima has also reported during the Parliament Session that after the strengthening the cybercrime unit in the country, the struggle has started yielding some fruits. About 320 people have been apprehended between July and December 2011. In 2012 about 320 people have been arrested as suspects over the crime.[4]

Reports also show that cybercrimes have occasioned great loss to the financial sector in the country. It is said that about Tshs. 1 billion / -Euro 8,897 and USD 551,777 have been stolen through cybercrimes, posing a big challenge to the government.

Due to the high technological advancement, many cases within and outside the country have been referred to the courts of law. The government has realized the trend being on the high increase and proceeded to enact the *Electronic and Postal Communications Act* (EPOCA) of 2010 as well as the Anti money laundering Act, 2006 to deal with cyber crimes. On top of that the government has joined efforts

[3] Cited at http:/allafrica.com/stories/201206270719.html.?aa-source=useful-column visited on 5th June, 2013 at 11.00am

[4] http://dailynews.co.tz , visited on 7th June, 2013.

with the Police Force, the Tanzanian Revenue Authority (TRA), Financial Institutions, the Media and the Tanzania Communications Regulatory Authority (TCRA) to educate the general public on what the crime is and how the same can be fought.[5]

The relevant Ministry, through the Police Force, in ensuring that the fight to combat cybercrimes is enhanced has trained 250 police officers and have been distributed through the regions. The financial institutions have made sure that their password security system is tightened.

It has also been reported that there are the ongoing efforts by the Government to ensure that there is a cyber law in the country which shall address the ever increasing incidents of cyber frauds and crimes. Presently, computer emergency response team has been formed to respond to cyber –related crimes. In the meantime, the government is also considering working further on the National ICT Policy of 2003 to ensure that all new developments in the industry are accommodated. This was said by an expert of cybercrimes in Dar es Salaam when presenting a paper at the National Internet Governance Forum (NIGF) which is a multi stakeholder's forum that discusses various issues related to governance of internet. This contains members from the government, the civil society, academicians and technical experts.[6]

About 10,000 kilometers fibre optic cables of the National ICT Broadband

[5] Ibid.
[6] http://dailynews.co.tz , visited on 6th June, 2013

Backbone (NICTBB) have been laid down countrywide. Dar es Salaam alone, 90 kilometers have been covered by the NICTBB whereas cross-border connectivity to other eight neighboring countries has been implemented. This places Tanzania among leading countries in Africa which has been covered by the optic –fibre cables. This being the case, the country is provided with extra required broadband facility. All higher learning institutions, secondary schools, primary schools and hospitals throughout the country, through the multi- millions state funded project will obviously be connected to the national backbone as the country embarks on embracing e-learning tele-medicine and e-governance.[7]

Despite the high rising of cybercrimes in the country, unreliable electricity and limited coverage of connectivity, the national backbone has set opportunities for social and economic growth in the country.[8] There is also a high increase use of e-banking by commercial banks in the country and other computer –based transactions. These have fueled the high rise of cyber crimes which in actual facts are more complicated in investigations and prosecutions. The Director of public Prosecutions (DPP) Dr. Eliezer Feleshi averred that the offences involving hi-tech includes money laundering and financial terrorism. In essence all transactions nowadays are taking place online, without physically seeing the person. That being the case, criminals have found the internet less controlled and see it a free place where they are capable of committing crimes anonymously.

However it has been stated that in order to combat cybercrimes, working as a team

[7] http://dailynews.co.tz , visited on 7th June, 2013
[8] Ibid.

is of paramount consideration.[9]For the purpose of this work much emphasis therefore, will be on the elimination of cyber crimes in Tanzania, the struggles, the law and the practice there of.

The previous paragraphs sought to show that with the advent of electronic communications in the country, the use of e-money, e-banking, sms, MMS and other communications done through electronic devices like mobile phones, Ipads, Computer and Automated Teller Machines (ATM) a few to mention have fuelled the high rise of cybercrimes. The big challenge of hi-tech is computer crimes as shall be discussed at length in this study. The technology has brought fundamental challenges and changes on the way things take place in the country. The legal regime is also challenged in one way or another. This work shall deal mostly on the role of the legal regime in eliminating cybercrimes in the country.

1.2 Statement of the Problem

Despite the development economical and social brought by the use of the internet and e-commerce, it has emerged electric crimes or computer crimes or cyber crimes as famously known. There is a tremendous growth of cyber crimes in the country whereby consumers online are at stake. This work critically reviews the legal framework on cyber laws in Tanzania and sees whether the same has addressed cyber crimes adequately. In other words, it seeks to answer is this: Does the existing legal framework able to combat computer crimes and cyber fraud?

1.3 Objectives of the Study

[9] Cited from http://allafrica.com/new/group/main/main/id/00021259.html? aa-source = useful.com

The study aims at tracing the genesis of computer crimes in Tanzania and the struggles to curb or eliminate them using the legal framework. The research at hand shall undertake to review the role of law in combating electronic crimes in Tanzania to ensure that online consumers are legally protected. The work at hand will also assess the efficacy of the legal framework in combating cybercrimes in Tanzania. The research will dissect and see whether cyber crimes in the country can well be eliminated just by use of legal framework or other measures on top can be improvised to ensure that cyber crimes issues are addressed in broader context.

The work shall also assess the role of the legal profession in addressing cybercrimes and their challenges thereto. In the final analysis, the research shall accordingly advise what should be the way forward. By so doing the work shall contribute to the existing body of knowledge in the country on cybercrimes.

1.4 Significance of the Study

This study has the following significance:-

i. The study at hand will enrich the existing body of knowledge about cybercrimes in Tanzania.
ii. The findings obtained through this study will benefit the legal fraternity and the public at large by letting them know what cyber crimes are, what are the challenges and the remedies pertinent to cyber crimes and the legal frame work there to.
iii. This study reviews and assesses the legal regime on cybercrimes in the country and sees whether the same is adequate or not. The study also

observes and recommends what should be done based on best lessons from other jurisdictions with a suitable legal framework to combat cyber crimes.

iv. This study also assesses the impact of cyber crimes on social economic status of the country.

v. Last but not the least the study undertakes to address how online consumers should be protected against cyber crimes. What steps to be taken to ensure the online users are well protected?

1.5 Hypothesis

This study is built on the hypothesis that the increasing rates of incidents of cyber crimes in Tanzania can only be combated by an adequate and efficient legal framework.

1.6 Literature Review

Various writers have written on cybercrimes and this section seeks to review only a few which are directly connected with the problem under investigation in this study. After the review, the researcher will be able to show the existing gap which this study seeks to fill.

One such author is Mwiburi, A.J.[10]. who argues that the EPOCA which was meant to address almost all electronic issues and communications in the country has fallen short of this intention. He is further of the view that cybercrimes are intermingled with electronic commerce like e- signature, digital signature, digital devices and e-

[10] Mwiburi, A.J., " Legal Implications of Developments in Information and Communication Technology: An Appraisal of the Electronic and Postal Communications Act, 2010 in relation to cybercrimes in E-Commerce in Tanzania"

contracts and that they ought to have been addressed because they are very important. He concludes that legal regime in Tanzania in respect of cyber crimes is still wanting in that EPOCA did not address all the issues important to cybercrimes, hence, inadequate because it leaves a big lacuna in the legal regime on cybercrimes.

Another writer is Heath cote, P.M.,[11] who discussed various issues on ICT generally. He discusses the role of ICT technologies in business and commercial transactions and developments. He further, discusses the role of ICT in manufacturing industries, taking care of the society and educational developments. On top of that, computer crimes are discussed on the purview of the *United Kingdom Computer Misuse Act*, 1990 and the *Data Protection Act***,** 1984.[12] He further advises some measures to be taken in order to protect ICT systems against illegal access and damages. Such measures she proposes are physical restrictions, encryptions and software usage. Even though Heathcoat advances useful techniques to ensure security to ICT devices; she falls short on what can be done in respect of the legal framework.

Gunarto, H.,[13] discusses ICT security on ethical perspectives and scientific efforts done to ensure that data are well protected. This protection should be done by encryptions, back ups, fine walls, physical restrictions, a few to name. He gives more emphasis that ethical issues or values need be adhered to, in order to ensure that data and information are well protected. He also discusses how important are the agencies mandated to watch on information security and the importance of

[11] Heathcote,P.M., As Level ICT,Payne-Gallawary Publishers,Ipswish,pg 2-28
[12] ibid
[13] Gunarto ,H., Ethical Issues in Cyberspace and IT Society Ritsumeikan Asia Pacific University

having new codes of ethics. He also discusses some legal issues on cybercrimes like jurisdiction, the criminal intent (*mens rea* and *actus reus)* and how the same aids in the commission of crimes.

Sigh, Y.,[14] discusses various issues of cyber laws such as intellectual property rights in cyberspace, computer software and Patent information Technology Act among other things. On computer security, he discusses in detail the use of digital signatures basing on public key and encryption using numbers. He also discusses on security concerns in which case he suggests that law should be used to enhance security. He furthermore, suggests that there should be an appointed controller on the use of electronic signatures and certificates.

Ubena, J.[15] discusses at length on the pace of ICT developments in Tanzania and argues that in the wake of convergence on various ICT technologies, Tanzania is in the dire need of having comprehensive electronic communications legislation.

Viswanathan, A.,[16] has also discussed on cybercrimes or computer offences among many issues. He elaborates what are cybercrimes and continues to mention and explain them being hacking, bots and BOTNETS, key loggers, website defacement, malware-viruses, phishing, distributed denial of services, fishing, pharming, identity theft, spoofing, rootkits, mobile malwares, spams, to mention a few. He discusses also on electronic signatures, data Protection and privacy obligations, obscenity and

[14] Singh,Y., ''Cyber Laws,'' 5th Edn,New Delhi: Universal Law Publishing Co.Pvt.Ltd., 2012

[15] Ubena, J. "Why Tanzania Needs Electronic Communication Legislation? Law keeping up with Technology" The Law Reform Journal, Vol 2, No.1, 2009, pg.21

[16] Viswaanathan ,A.,Cyber Law,Indian and International Perspectives on Key Topics Including Data Security,E-Commerce,Cloud Computing and Cybercrimes, Lexis Nexis Butterworth Wandwa,Nagpur,2012

child pornography, liabilities of intermediaries, government interceptions, monitoring and decryptions and enforcement issues on institutional framework. Carol, J.M. has also discussed at length the issues on computer crimes and security[17] While carol analyses computer security premising his approach on physical and technological measures, the work at hand endeavors to discuss computer security on legal perspectives and challenges thereto. Daid, L.C[18] argues that, as computer crimes become more prevalent, there is also a dire need for police personnel and those without computer expertise to be trained in order to have an understanding of various basics in computer technologies.

Mambi, A.[19] is of the view that there is a big relationship on cybercrimes, privacy issues and data protection, child grooming and cyber –stalking. He asserts that computer technology has transformed the production of child pornography into a very sophisticated global industry and electronic communications has made it possible and easy to send and receive pornography. Children are therefore targets and vulnerable to child sex exposed through pornography, Invasion of privacy and online fraud, file sharing abuse (peer 2 peer), illegal advertisements and e-gambling. Like the other writes, he shares the views that it is difficult to prosecute, arrest crime offenders of cybercrimes. The guiding questions are which country has the right to arrest e-crime offenders and prosecute under the cyber space? Which court will have jurisdiction?

---

[17] Carol, J.M, "Computer Security", Butterworth's and Company, London, 1977, pgs 81- 121

[18] Daid, L.C, Computer crimes categories: How Technology Criminals Operate, Michigan state University, East Lansing Michigan

[19] Mambi, A., shaping the information society, e-children protection, legal measures, a paper presented at IGF, 2nd Parliamentary Forum

Bain Bridge, D.[20] discusses at length the development of computer technology and the implications thereto. He points out that computer crimes or cybercrimes is a big issue in United Kingdom as per the survey done in 1999. The percentages traced were alarming as follows:- Pornography was 40%, hacking was 9%, viruses was 41% and fraud was 10% 45. Nevertheless, Brainbridge discussion concentrates in UK and EU jurisdiction and laws. This study at hand endeavors to assess and discuss the cyber crimes in Tanzania, though the UK and EU experiences are very helpful when assessing the Tanzanian context.

Another writer is Comer, M.J.,[21] who asserts that some people discuss and suggest that each and everything, save for most technical explanation, need to be left out when defining computer crimes. In his views, computer fraud is all about any financial dishonest taking place in a computer environment.

Lloyd, I. J.[22] discusses the development of ICT by tracing it back about five thousand years when there was an invention of the abacus. Lloyd argues that computers have not been regulated seriously because were considered that, their use was for mathematical purposes only. As time went on concerns on regulating computer started to carry legal importance when digitization started changing data into a commodity. Furthermore, Lloyd discusses relevant aspects of e-commerce, like e-contracts, e-taxation and computer crimes. Despite the fact that his analysis is United Kingdom based, it is very important and worthy of consideration in the study

[20] Brainbridge, D. , "Introduction to Computer Law, Pearson, Education London , 5th Edn, 2004 pg 1
[21] Comer , M.J. , Corporate Fraud, Mc Graw Hill Book Company, 2nd Edn, London 1985 pg 40.
[22] Lloyd, I. J., Information Technology Law, Butterworth 3rd Edn, London, 2000 pg 1

at hand.

The above reviewed literature shows that different authors have addressed and discussed the issues in relation to cyber crimes on various perspectives and dimensions. Nevertheless, no one has addressed the ICT issues in the light of cybercrimes in Tanzania, assessing the law and practice thereof. This study endeavors to assess critically on the legal regime in Tanzania and proposes some solutions.

1.7 Research Methodology

1.7.1 Area of Research

The study at hand has been mainly conducted in Dar es Salaam. The rationale behind this is that Dar es Salaam is a commercial city and many transactions are done in Dar es Salaam. Dar es Salaam is a hub as considered by many for the reason that all commercial communications, transactions, government Ministries headquarters are located in Dar es Salaam. The research preferred the City for purpose of convenience and availability documentation centers as well as experts for consultation purposes.

1.7.2 Field Research

In this category, the researcher employed the three traditionally used methods such as questionnaires, interviews and observation. Due to time constraints encountered by the researcher, she decided to unstructured oral interviews to give more flexible and user friendly environment to collect data, and since the study relates to different fields, different respondents of diverse educational background were interviewed.

These are lawyers, engineers, police officers, accountants, computer analysts, judicial officers and telecommunication experts.

The researcher interviewed Resident magistrates at Kisutu Resident magistrate Court in Dar es Salaam, an advocate of the High Court of Tanzania specializing in ICT Laws, a graphics designer and computer programmer, Director of Legal services at Sumatra, IT specialist at Bomora Attorneys, Members of Parliament for Tandahimba who is a lawyer on ICT Laws, Head and Director of Risky Management at PPF, Director of Legal services PPF, District Magistrate Karatu District Courtt, Karatu Arusha, the head of cyber crime Unit at the Police Force Head quarters, Dar es Salaam, six computer users, three from Sophy Internet café Mabibo Dar es Salaam and three users from Bamora Attorneys Law office.

When administering questionnaires, conducting interviews with various respondents as already submitted above, the researcher managed to observe the magnitude of the problem in the country. Respondents were concerned and wanted the problem to be addressed. They gave the researcher full participation during the interview and administration of the questioners. This helped the research to get useful information.

The researcher used this combined approach to ensure that data collected were collected from different perspectives and reflected what is happening in the field. This strategically employed has yielded fruits giving a balanced data collected by the researcher. In this respect, 70% of the planned oral interviewees were reached, whereas 20% of the respondents were administered with questionnaires and

responded in time. It is obvious that an interview was a success rather than the questionnaire method. All in all both were used to collect data and bring this study into a success.

1.7.3 Library Research

Traditional based libraries were visited by the researcher to enhance data collection. The rationale behind such approach was to ensure that the relevant literatures pertinent to this study were reviewed. The researcher visited the University of Dar es Salaam Library, the Open University of Tanzania Library, the school of Law Library and Tanganyika Library. Nevertheless, the researcher visited various online sources as shown in this report where she managed to trace e-books, journals, case books, directories , a few to name. All these were meant to enhance this study.

1.8 Scope of the Study

Collected data covered the period before the enactment of *Electronic and Postal Communications Act,* 2010, the Money Laundering Act 2009. The legislations were enacted meaning to address electronic communications though fell short of the intention. Geographically, the research has been conducted in Dar es Salaam City, the commercial hub where many transactions are carried out. According to the research problem, various respondents of different professions were consulted. The Research was limited between the months of June, July & August, the year 2013.

1.9 Limitation of the Study

While carrying out this study the researcher encountered a number of difficulties. The researcher started her study a bit late because she had family issues to sort out;

attending the sick father who passed away just prior to the beginning of the research was not a small thing. The incident drained her energy physically and psychologically. The researcher had to meet all family issues, study and research, at the same time work out and perform well as a Magistrate. Another challenge was the go and come back for administering and collecting back the questionnaires. This made the researcher not to meet all the targeted respondents.

Financial constraint was another challenge faced by the researcher. It was not easy to move from one place to another with a very limited self sponsored budget. Nevertheless, the researcher with self sacrifice and commitment, good management of time and well arranged financial plans, was able to make this study a success.

1.10 Conclusion

Chapter one was an introductory chapter laying down the theoretical framework of the study. Background to the problem, statement of the problem, study objectives, literature review, hypothesis, research methodologies and significance have been discussed at length in this Chapter.

CHAPTER TWO

2.0 THE NATURE OF CYBERCRIMES WITH REFERENCE TO THE FINANCIAL SECTOR

2.1 Introduction

Lloyd correctly to my view points out that criminals have taken advantage of the development of computer technologies to perpetrate their ill-motives and that with the usage of the internet in the banking sector, financial institutions have become constant targets of fraudsters.[23] It is for this reason that this Chapter is intended to focus on cybercrimes in the financial sector.

2.2 The Nature of Cybercrimes

2.2.1 Overview

It is true that the enormity of cyberspace is stretching the boundaries of the possibility of attacks worldwide in that the cybercrime is committed by the criminals in different jurisdiction through Cyberspace. The term cyberspace was first coined by the author William Gibson in his sci-fi novel Neuromancer (1984) as

> *"A metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require*

[23] Lloyd, I. J., *Information Technology Law*, 6th ed, Oxford University Press, 2011, p.210.

any physical movement other than pressing keys on a keyboard or moving a mouse.[24]"

Basing from the above given description it may be noted that the virtual world provided by cyberspace movement is borderless in nature that the "www" access does not require any physical movement or cross border customs checks but rather transitional communication with different people in different countries, whereby this communication or actions are made by simple click on the mouse or keyboard and any such communication can travel from one country to another within minimum time frame.[25] Through the use of this virtual world, some people may use the cyberspace for better and lawful purpose while others use it for ill motive to commit illegal acts or to gain a certain economical advantage, this leads to the commission of crimes of which these days are technically referred as cybercrimes as explained hereunder.

Cybercrime can be explained in various words such as crimes that can be committed with the use of a computer and the Internet. Some define it as crimes committed on the internet using the computer as either a tool or a targeted victim.[26] From these definitions cyber crime can be looked in a narrow perspective and in a wide sense. Cybercrime in a narrow sense covers any illegal behavior directed by means of electronic operations that targets the security of a computer system and the data processed by them. In a broader sense (computer crime) covers any illegal behavior committed by means of or in relation to computer system or network,

[24] Gavazos, E. A., *Cyberspace and the Law,* Cambridge-London, 1996, p. 1
[25] See also Bajaaj, C. N., *op.cit.,* p. 282.
[26] Ibid, at p. 285

including such crimes as illegal possession and offering or distributing information by means of computer system or network.[27]

Thus Cybercrime is any activity in which computers or networks are a tool, a target or a place of criminal activity and as hinted above it are committed through cyberspace.[28] Therefore cybercrime can be simply referred as electronically committed crime through the use of Computer and internet and this being the case it is very difficult to apprehend the criminals when they are committing and it is also difficult to trace the perpetrator of the offence and where about because the offence is not a physical offence for which the perpetrator can be easily recognized and arrested.[29]

Cyber crimes can be committed by individuals inside and outside the system. External individuals may have unauthorized access to the system through, for example hacking[30], sniffing[31], spoofing[32] and denial of service[33] attacks expose banks to new security risks.[34] Open electronic delivery channels have created new security issues for banks with respect to confidentiality and integrity of information, non-repudiation of transactions, authentication of users and access control.[35]

---

[27] Ibid.
[28] See Prasana, A., "Cybercrime: Law and Practice" accessed at http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf
[29] Bajaa, K.. K. & Debjani, N., *op.cit.*, at p. 282.
[30] Hacking refers to the practice of breaking into a computer without authorization, for malicious reasons, just to prove it can be done, or for other personal reasons.
[31] Sniffing involves the use of software program that is illicitly inserted somewhere on a network to capture (sniff) user passwords as they pass through the system.
[32] Spoofing refers to an attempt to gain access to a system by posing as an authorized user.
[33] A denial of service attack represents an attempt to overwhelm a server with requests so that it cannot respond to legitimate traffic.
[34] *Ibid.*
[35] *Ibid.*

Frauds and theft is said to be a breach to the security system of financial institutions' payment systems, which may have adverse affects on individual accounts or threaten institutions or networks.[36] The Federal Reserve Bank of Atlanta underscores the fact that industry statistics show payment fraud continually evolving, which is a likely reason it will never disappear and that institutions prefer to incur losses associated with fraud rather than paying the price of preventive measures.[37]

Fraud is not new to banks. Consumers transacting banking business in electronic form are likely to face problems that their counterparts transacting paper-based banking business face.[38] The difference is that e-crimes are committed in the digital environment. However, it is argued that theft is theft regardless of whether it is digital theft or traditional theft.[39] The M*odus operandi* has changed with the digital capabilities enhancing the speed, reach, and magnitude with which these crimes are executed.[40]

There is no need for thieves now days to use a gun and physical presence in a branch to rob banks. It is disgusting to learn that, fraudsters use the same technologies that enable electronic payment innovations to perpetrate criminal

[36] Gibbons, J. H., "Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity", U.S. Government Printing Office, Washington, D.C. 20402.
[37] See an Article "Fight against payments fraud: The target is moving, but no everybody takes aim' accessed at http://portalsandrais.frbatlanta.org/online-banking-fraud/
[38] See also Loudon, K.C. & Traver, C.G., *op.cit*., at p. 262.
[39] *Ibid.*
[40] Kondabagil, J., *op.cit.,* at p. 93

intents, like identity theft and payments fraud.[41] They only need access to a networked computer giving rise to risks of transacting with unauthorized or incorrectly identified individuals in an electronic banking environment, the apparent consequences being financial losses to both customers and banks through fraud.[42]

There are numerous ways in which criminals have exploited the vulnerabilities in the open networked environment of e-banking and committed frauds.[43] Even systems closed networks have occasionally been targets of criminal attacks. From this analysis, two major categories of frauds can be made. These are card-based fraud and network-based fraud.[44] The section below attempts to give a detailed discussion on these ways in which fraud can be committed. Where possible, statistics to support the discussion will be given. It should however be pointed that, a discussion on types frauds can only a discussion towards a very controversial issue – how are issues related to liability for losses handled.

2.2.2 Card-Based Fraud

Igor Pipan[45] points out that the vast growth of the payment card industry (PCI) in the last 50 years has placed the industry in the centre of attention, not only because of this growth, but also because of the increase of fraudulent transactions.[46] Despite these efforts, it is on record that in UK alone cash machine fraud losses totaled £

---

[42] *Ibid.*.
[43] *Ibid.*
[44] It is always safe to classify frauds in e-banking due to the fact that as technology advances, criminals also forge new ways of committing fraud.
[45] Pipan, I, *The Role of IT/IS in Combating Fraud in the Payment Card Industry*, accessed at *www.arraydev.com/commerce/jibc/* .
[46] *Ibid.*

36.7 in 2009.[47] The European Commission reports estimated credit card fraud in European Union is between €500 en €1000 million.[48]

The UK Payment Association recognizes five types of card-based fraud: [49] firstly, lost/stolen credit or debit card where the card is lost or stolen and then used by an unauthorized individual. Secondly, mail non receipt where the card or cards are being intercepted while being sent to the cardholders by post. Thirdly, counterfeit which is the type of fraud same as skimming, where the card information is copied from the magnetic stripe. Fraudsters often skim cards by using a device that is fitted to a cash machine or a PIN pad. This data is then transferred onto a fake magnetic stripe card and used in countries that have not yet rolled out chip and PIN.[50] Fourthly, card not present where the account information from the card is used to make unauthorized purchases over the telephone or the internet, and lastly, card ID theft where the account information is stolen by unauthorized individuals to make fraudulent purchases and can take many different forms.

Fraudsters can as well access the card systems and copy information that they may use to access customers' funds. In 2009, 60 percent of identities exposed were compromised by hacking attacks, which are another form of targeted attack.[51] The

[47] The source of this information is http://www.link.co.uk/Press/NewsReleases/Pages/Fraud_Prevention_Guide.aspx
[48] APACS, 2008; FPEG, 2009; European Commission, 2008. *JIBC December 2009, Vol. 14, No. 3*
[49] The source of this information is http://www.ukpayments.org.uk/payments_industry/payment_fraud/plastic_fraud/types_of_card_fraud
[50] *Ibid.*
[51] Symantec Global Internet Security Threat Report: Trends for 2009 Volume XV, Published April 2010accessed on http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

majority of these were the result of a successful hacking attack on a single credit card payment processor. The hackers gained access to the company's payment processing network using an SQL-injection attack. The attackers then installed malicious code designed to gather sensitive information from the network, which allowed them to easily access the network at their convenience. The attacks resulted in the theft of approximately 130 million credit card numbers. An investigation was undertaken when the company began receiving reports of fraudulent activity on credit cards that the company itself had processed. The attackers were eventually tracked down and charged by federal authorities.[52]

2.2.3 Network-Based Fraud

It was pointed out earlier in this Chapter that, existing banks with physical offices, ordinarily termed as 'brick-and-mortar banks, are establishing websites and offering internet banking to their customers in addition to their traditional delivery channels. There are also those banks which offer 'internet only' banking services with the data centre or some other location serving as the legal address. These banks allow customers with the ability to make deposits and withdrawals via ATMs or other remote delivery channels owned by other institutions.

Customers may also make use of their debit and credit cards when paying goods and services in face to face, internet or telephone. For law-abiding citizens, the internet holds the promise of a huge, convenient, global marketplace, al at a bargain price. For criminals, the internet has created entirely – and lucrative-ways to seal from the

[52] *Ibid*

more than 1 billion consumers in the world over the internet.[53] According to Singh, [54]steep rise in online banking fraud has undermined its success as few bank customers want to return to boring bank queues for secure transactions.

Internet banking fraud is fraud or theft committed using online technology to illegally remove money from, or transfer it to, a different bank account. [55] The risk on the internet being used in effecting payments lies on its nature.[56] Loudon & Traver[57] underscores the fact that the internet was never designed to be a global marketplace with a billion users, and lacks many basic security features found in older networks such the telephone systems. It is open and vulnerable by design.[58] The communication path is very complex and it may include passing through several public servers, lines or devices between the customers personal computers and the bank's internal networks.[59] The Reserve bank of India's Report on Internet Banking (2001) outlined some distinctive features of the Internet.

First, it removes the traditional geographical barriers as it could reach out to customers of different countries/legal jurisdictions. This has raised the question of jurisdiction of law and / or supervisory system to which such transactions should be

---

[53] Loudon, K. C. & Traver, C.G., E-Commerce: Business, Technology and Society, 4th Edn, 2008, Person Education International, New York, p. 257.
[54] Singh, N. P., Online Frauds in Banks with Phishing, *Journal of Internet Banking and Commerce*, August 2007, vol. 12, no.2 (http://www.arraydev.com/commerce/jibc/)
[55] http://www.afp.gov.au/national/major_fraud/internet_scams
[56] Kondobagil, J. (2007), *Risk Management in Electronic Banking; Concepts and Best Practices*, John Wiley & Sons (Asia), Pte Ltd: Singapore, at p. 21.
[57] Loudon, C.K. & Traver, C.G., *op.cit.*, at p. 257.
[58] *Ibid.*
[59] *Ibid.*

subject.[60] Second, it has added a new dimension to different kinds of risks traditionally associated with banking, heightening some of them and throwing new risk control challenges. Third, security of banking transactions, validity of electronic contract, customers' privacy, etc., which have been traditional banking concerns have assumed different dimensions given that internet is a public domain, not subject to control by any single authority or group of users.[61] Fourth, it poses a strategic risk of loss of business to those banks who do not respond in time, to this new technology, being the efficient and cost effective delivery mechanism of banking services. Lastly, a new form of competition has emerged both from the existing players and new players in the market who are not strictly banks as several policy decisions have also been made.[62]

As will be shown below, threats in security of electronic payment systems at the global level are alarming, despite efforts employed by banks to minimize security breaches. For example, in 1995, $10 million computer fraud against Citibank was the first successful penetration by a hacker into the system which transferred trillions of dollars a day around the world. Of the $10 million dollars illegally transferred, $400,000 was not found.[63]

Hi-tech fraudsters have urbanized a new way of tricking on line banking customers.

[60] See the Reserve bank of India's Report on Internet Banking (2001)
[61] *Ibid.*
[62] *Ibid.*
[63] Yang, *(supra).*

One such most well known and fast growing technique is phishing.[64] It is derived from fishing. Phishing (also called brand spoofing) is a term used for a short of fraud where phishers send out spoof email to a random database to fool the recipient in to divulging personal information like credit cards details, usernames and passwords, that can be used for identity theft.[65] Phishing is one of the most well known and fastest growing scams on the Internet today.[66]

According to Singh,[67] the typical phishing scam involves an e-mail that appears as though it came from a reputable and known service institutions or company. The e-mail appears to be legitimate and the actual one. The message generally indicates that, due to problems in the institution (bank in this case) such a database updates, problem occurred in server, security/identity theft concerns, the recipient is required to update personal data such as passwords, bank account information, driver's license numbers, social security numbers, Personal Identification Numbers (PIN), and so forth. The e-mails include warning to the users that failure to immediately provide the updated information will result in suspension or termination of the account.[68]

Latest in phishing is application of Trojan horse program. Trojan horse" program insinuates itself into a user's computer via an email and directs the user of the system to website which is exactly similar to financial institution web site. Crooks

[64] Sigh, N. P., "Online Frauds in Bank with Phishing" *Journal of Internet Banking and E-Commerce,* August 2007, Vol. 12, no. 2.
[65] *Ibid*
[66] *Ibid.*
[67] *Ibid.*
[68] *Ibid.*

pick up passwords and account numbers as soon as customer logon to these sites.[69] In 2009, the financial sector remained the sector most heavily targeted by phishing attacks, accounting for 74 percent of the brands used in phishing campaigns. Analysis of the data for phishing websites in 2009 indicates that the financial services sector also accounted for 78 percent of that total, which was slightly higher than 2008, when the volume of phishing websites for financial services was 76 percent.[70] Again, in 2009, the top two brands phished belonged to the largest U.S.-based multinational banks. In 2008, these brands ranked 17th and seventh in 2008, respectively. There was nearly a sevenfold increase in phishing URLs that targeted the top-phished brand in 2009 over the previous reporting period, while the second-ranked brand had almost a threefold increase. This indicates that phishers are narrowing their focus. Rather than targeting a wider range of smaller financial institutions, they are specifically targeting the largest banks that are more likely to have a higher number of customers banking online.[71]

In the recent past, according to the UK payments association Apacs,[72] the huge rise in online banking fraud coincides with an upsurge in the number of phishing scams being run on the web and demonstrates the importance of educating bank customers about this type of crime. The similar concern is raised by Financial Services Authority (FSA), UK regulator. FSA recorded 8.000% increase in online banking frauds and identified phishing as major instrument. With the growth of phishing customers are realizing that online transactions in particular e-commerce

[69] *Ibid.*
[70] *Ibid.*
[71] *Ibid.*
[72] The source of this information is http://www.bcs.org/server.php?show=conWebDoc.10452.

transactions are not safe.[73] Globally, about 30,000 phishing attacks are reported each month, of which over 80% are directed at financial institutions.[74] Phishing attackers have targeted at financial entities such as Citibank, Wells Fargo, Halifax Bank, eBay, and Yahoo as reported by Secure Science Corporation (2003).[75]

In the UK alone, the number of recorded phishing incidents was 312 and 5059 between January to June, 2005 and January to June 2006 and it was among top 10 phishing site hosting countries from Jan 2005 to Jan 2007.[76] The amount of cash stolen in the first half of 2006 was £23.2m, the committee was told, and was likely to be £22.5m in the second half of the year.[77] Singh points out US as leaders of top 10 phishing sites hosting countries and also experienced large number of phishing attacks.[78] At least 1.8 million consumers had been tricked into divulging personal information in phishing attacks, most within the past recent years.[79] The average loss per phishing attack was $1,244 in 2006, up from $256 in 2005.[80]

In an interesting case in the United States, Joe Lopez,[81] a Miami businessman who regularly conducted business over the internet, sued Bank of America at the Miami Circuit Court for negligence and breach of contract for failing to provide protection for online banking risks that the bank was aware of. On 6th. April 2004, his computer system was hacked into and US$90,348.65 was wired from his account at

[73] Singh, *Op. Cit.* at p. 2.
[74] *Ibid.*
[75] *Ibid.*
[76] *Ibid.*
[77] *Ibid.*
[78] *Ibid.*
[79] *Ibid.*
[80] *Ibid.*
[81] See Alho Inc. v Bank of America (2005), Miami Circuit Court (Unreported).

Bank of America Direct, its online portal, by Latvian cyber criminals, to Parex Bank, a bank in Riga, Latvia without his approval. About US$20,000 of the money was withdrawn before the account was frozen by the Latvian bank. A subsequent Secret Service investigation requested by the bank detected the presence of the *'coreflood keylogging Trojan'* on his computer.

Lopez claimed that Bank of America had knowledge of the Trojan horse virus known for infiltrating and compromising security systems and enabling unauthorized access to infected computers, and therefore the bank had a responsibility to inform its customers of the virus. Further the bank should have been alerted when the transfer of such a large sum to Latvia was initiated. Latvia, along with Russia, Eastern Europe, and the other Baltic states is known for having a high level of cyber-criminal activity and thus a large monetary transfer to that part of the world should have been questioned by the bank.

To make matters worse the bank failed to act upon being notified within minutes of the unauthorized transaction and refused to assist in liasing with the Latvian bank to freeze the monies or release the balance to Lopez. It was only in July 2004, that the bank sent a letter to its users alerting them to a new "dual administration" feature requiring the approval of at least two individuals to execute a funds transfer. The letter also recommended that clients install antivirus software. Bank of America denied liability for the loss since its systems were not hacked into and all appropriate measures were taken to complete the transfer.

2.2.4 Banks' Employees Fraud

Employees of the institution are frequently the source of electronic banking crime. [82] They are likely to have access to the systems and often can mask criminal actions behind legitimate activities. They may hide unauthorized procedures within programs (the "Trojan horse" strategy) by building in instructions to abort or divert authorized transactions, and then remove this procedure from the computer's memory bank[83]. Unauthorized copying of either programs or data, such as account numbers and personal identification numbers (PINs), usually cannot be detected or traced.[84] It is for this reason that many incidents of e-crimes are difficult to detected when they are committed by insiders, who have a good understanding of the systems and controls and are thus able to exploit the loopholes without leaving trace.[85]

Talwar[86] recounted a reported incident of an IT expert who could penetrate the multilayer password system governing the fund transfer facility of the bank, which was allowed to be self-operated by its corporate customers. He could successfully effect wire transfer of millions of dollars from a corporate account to his own / wife's account across continent to a destination in Europe. Though the corporate treasury manager of the customer was watching the fund transfer stolen and shifted before his very eyes, he was helpless in the context of such operation happening in

[82] *Ibid.* This view is widely supported by various authors , the Basel Committee and the Reserve Bank of India Report on Internet Banking. There is also enough evidence from the field survey that employees of a number of banks take part in committing crimes.

[84] *Ibid.*

[85] Talwar, S. P. "Computer Crime - an Overview" Accessed at http://rbidocs.rbi.org.in/rdocs/Bulletin/DOCs/6270.doc

[86] Talwar, S. P. "Computer Crime - an Overview" Accessed at http://rbidocs.rbi.org.in/rdocs/Bulletin/DOCs/6270.doc

few seconds. While the cyber reach was possible in seconds, the efforts of law enforcement took time to cross the continental legal and criminal enactment barriers to overcome before they could ultimately nab the above criminal.[87]

In Nigeria, 600 Euros Electronic Funds Transfer fraud perpetrated through a bank in Benin, Edo State. The amount was sent by an Irish businessman, Kevin Fuller, to his Nigerian partner through Western Union Money Transfer at 5.28pm Nigerian time on 3rd November 2008 from Dublin Ireland. The money was collected by a yet to be identified person at exactly 6.22pm Nigerian time on the same day. The inward transfer and outward payment took place after 4pm when banks had closed their doors to outside customers.

2.2.5 Money Laundering Using Electronic Banking

The offence of money laundering is now being committed using computers and computer networks, the internet inclusive. The imminent danger with the use of the internet is that transactions become instantaneous, untraceable and may easily be anonymous, leaving no audit trail.[88] As shown below, the use of computer technologies to perpetrate the offence of money laundering is currently not a new thing in Tanzania.

2.3 Incidents of Frauds and Unauthorized Transfer in E-Banking in Tanzania

As pointed out earlier in this study, clear manifestations of breach of security in e-banking include frauds, identity theft and unauthorized access to customers' accounts leading to unauthorized transfers of funds. A few incidents of fraud,

[87] *Ibid.*
[88] The Reserve Bank of India, "Internet Banking Report" op.cit., at p. 81

unauthorized transactions and identity theft that occurred in Tanzania show that Tanzania is not an island. The process of stealing money or property by using computer is called computer fraud which can be done in two ways.[89] The first is by using a forged bank card, and the second is by giving instructions to the computer to transfer funds from one bank account to another.[90]

The reasons for the increase of frauds in the banking sector include presence of unfaithful staff, lack of effective internal controls as well as willingness to share negative information among financial institutions and with law enforcers.[91] A few incidents below show that consumers transacting banking business in electronic environments face problems related to fraud leading to loss of their money.

There are a few incidents on unauthorized access to customers' accounts which were referred to courts of law. The first one involved one employee of the CRDB Bank together with another person from Mikocheni, Dar es Salaam. They were charged at the Kisutu Resident Magistrate's Court on 16th October, 2007[92] for allegedly committing the offence of stealing Tanzanian shillings 62, 000, 000/= through ATM machines using a debit card, branded "Tembo Card". At the time of writing this study, the case was still pending at the mentioned court.

---

[91] See the Speech by the Governor of the United Republic of Tanzania during an opening occasion of the Tanzania Bankers Association Workshop on Collaborative Approach in Combating Financial Crimes in the Banking Industry on 22nd July, 2010 in Dar es Salaam.

[92] The source of this information is a daily news paper called Habari Leo of 28th August, 2008 accessed at www.**habarileo**.co.tz/biasharaFedha/index.php?id=11715.

The second incident involved two Bulgarian nationals, Nedco Lazarov Stanchev and Stela Peteva Nedelcheva who were charged at the Kisutu Resident Magistrate's Court on 27th July, 2009 for forging an ATM card [93] contrary to sections 333, 335 (a) and 337 of the Penal Code[94] and stealing contrary to section 265 of the same law.[95] The accused persons were arrested following complaints by bank account holders that they were losing their savings in unauthorized ATM withdrawals.[96] A detective posing as a cleaner found a special device that the perpetrators had used to discreetly record people's Personal Identification Numbers (PIN).[97] Before they were arrested, the accused persons had already stolen Tshs. 14, 500, 000/= between 10th and 17th July, 2009.[98] At the time of preparation of the first draft of this study, this case was also pending at Kisutu Resident's Magistrates Court.

The third incident involved three accused persons, namely Akinlade Steve Ayorinde, Victor Mwombeki Rugarabawa and Alibina Anthoby Mushi.[99] In this case, the accused persons were charged with five counts of conspiracy to commit an offence of forgery contrary to section 384 of the Penal Code, Cap 16 [R.E. 2002] and four counts of forgery contrary to sections 333, 335(a) and 337 of the same law.

According to particulars of the offences, the accused persons forged four credit cards in Arusha and Dar es Salaam. The first visa card had numbers

[93] See the Charge Sheet filed by the Republic in Criminal Case No. 147 2009 accessed by the Researcher at the Registry of Kisutu Resident Magistrate's Court during a Field Survey.
[94] Cap. 16 Vol. 1 of the laws (R.E. 2002).
[95] *Ibid.*
[96] The source of this information is www.allafrica.com.
[97] *Ibid.*
[98] See the particulars of offence in Criminal Case No 147 of 2009.
[99] See Criminal Case No. 518 of 2010 pending before the Ilala District Court in Dar es Salaam. Records in respect of this case were accessed by the Researcher during the Field Survey at the Ilala District Court, Dar es Salaam on 8th July, 2013.

4434010000179843 which purported to have been issued by Cuscal Limited of New South Wales, Australia. The second visa card which purported to have been issued by Grow Financial Federal Credit Union of Tampa, Florida had numbers 4762070003614805. The third visa card had numbers 4559515000815914, which was purportedly issued by Chase Bank USA National Association of 2500 West Field, USA. The last visa card which purported to have been issued by the same Chase Bank USA National Association had numbers 4559592600486718.

The fourth occurred in 2009 when three businessmen and five officials of Barclays Bank were charged at the Kisutu Resident Magistrate's Court with conspiracy and fraudulently obtaining USD 1,081,263 (Tshs 1.43 billion), the property of Barclays Bank. [100] It was alleged that the accused forged two Society Worldwide Interbank Financial Telecommunication (SWIFT) messages purporting to transfer funds to Kigamboni Oil COM Limited.[101] At the time of writing this study, the case was still pending at the above mentioned Court.

As pointed earlier in this chapter, mobile banking is an innovation in Tanzania. Despite being a new distribution channel in Tanzania, fraudsters are increasingly using it to steal money from customers' accounts.[102] This problem is mostly common in NMB Mobile Banking.[103] Many customers using NMB Mobile have complained against unauthorized transfer of funds without their consent or

[100] See Daily News of 6th March, 2009, ISSN 0856-3812.
[101] *Ibid.*
[102] An interview with the NMB Bank Manager of Arusha
[103] NMB Mobile is a brand name of the mobile banking offered by the National Microfinance Bank.

knowledge.[104] The main reasons are negligence of customers in not keeping safe their cards and Codes and ignorance in using the ATMs to either withdraw or transfer money.[105]

A customer, for example, who has little or no knowledge in using an ATM may request another customer to assist. In the course of assisting him or her, he/she records the PIN as well as the number of the account and later uses these records to register in NMB Mobile as a genuine customer. He/she then transfers money from the customer's account to his own or some other person's account, after which he could now either transfer the money or withdraw using an ATM card.[106]

The customer may at a later stage discover that there is an amount of money or all the money in his/her account missing. In case he/she reports to the bank about the loss, the bank would at best assist him to trace the mobile phone number used to transfer the money. The customer would be lucky if the thief did not throw away or destroy the line he/she used. At times it proves very difficult to trace the person. In case efforts to trace the thief become successful, investigations leading to the thief being charged in Court would be made.[107] There are two incidents of theft using mobile phones that have been referred to a court of law. It should be pointed out that these are not the only incidents. There may be many others but the following two are used to justify the above contention.

An incident which occurred in Dar es Salaam in December 2010 is relevant to this

[104] Apart from cases in court, the source of this information is an interview with the NMB Clock Tower Branch Manager in Arusha held in July, 2010.
[105] *Ibid.*
[106] *Ibid.*
[107] *Ibid.*

study[108] In this incident, five University of Dar es Salaam students appeared before the Resident Magistrate's Court at Kisutu for allegedly stealing Tshs. 20,280,000 belonging to various customers using mobile phones.[109] Before the court, the prosecution alleged that the accused persons stole the amount of money belonging to two customers whose accounts were kept at NMB bank, Rufiji branch in the Coast Region, Tanzania. During the time of writing this study, the case was still pending at the court. Despite being newly introduced, the internet has also started being a target for crime. The CRDB internet banking system was recently used by one person to have unauthorized access to one customer's account maintained by the bank.[110] The customer was somehow negligent in keeping safe his user ID and the Password.

The criminal managed to transfer about 46, 000 USD to an account belonging to another customer of the bank, who, by the time he was arrested, had withdrawn about 40,000 USD. The case against him is pending at the Kisutu Resident Magistrate's Court. The criminal who transferred the money without authority of the owner was later arrested and after being questioned, admitted committing the crime.

Computers and computer networks including the internet are now used to commit the offence of money laundering.[111] The imminent danger with the use of the internet is that transactions become instantaneous, untraceable and may easily be

[108] See Tanzania Daima, ISSN 08562, January 27, 2011.
[109] *Ibid.*
[110] This was revealed during an informal interview with Mr. Charles Zabdiel Lawuo, a CRDB Lawyer
[111] The Reserve Bank of India, "Internet Banking Report" op.cit., at p. 81.

anonymous, leaving no audit trail.[112] The use of computer technologies to perpetrate the offence of money laundering is currently not a new thing in Tanzania. Several incidents that have been reported over the media and some which have landed to courts of law is evidence to this fact.

In July 2010, a number of cases on money laundering were filed in the Kisutu Resident Magistrates' Court in Dar es Salaam. A glance at these cases shows that the computer or computer networks facilitated commission of the offence to a large extent. The first case involved the *Republic v. Justice Lumima Katiti and 4 others*.[113] The accused persons in this case were charged with the offence of money laundering contrary to sections 3, 12(e) and 13(a) of the *Anti-Money Laundering Act*, Act No. 12 of 2006. It is detailed in the particulars of the offence that the accused persons transferred millions of money from several account numbers to other account numbers in diverse occasions.

Particulars of the ninth count in the charge sheet in the above case show that the accused persons transferred money from account No. 07410300033 of the National Bank of Commerce maintained by Excel Media amounting to Tanzanian Shillings nine hundred sixty million, one hundred forty eight thousand, two hundred ninety shillings and fifteen cents (Tshs. 960, 148, 290.15) to account Nos. 07413000112 of the National Bank of Commerce maintained by Express Booking Enterprises; 074103000276 of the National Bank of Commerce maintained by TAC Traders Limited and 074103000100 of the National Bank of Commerce maintained by Daima Pharmaceuticals while they knew or ought to have known that the money

[112] *Ibid.*
[113] See Criminal Case No. 149 of 2010.

was the proceeds of a predicate offence, namely theft, for the purpose of concealing the origin of that money or evading legal consequences of their actions.

The tenth count in the charge sheet showed that the accused persons transferred Tshs. 1, 426, 450, 680 to account number 074103000276 of the Nairobi Bank of Commerce maintained by TAC Traders Limited. The eleventh count showed that the accused persons transferred 1,415,418,801 to account numbers 07403000112 of the National Bank of Commerce maintained by Express Booking Enterprises, 074103000276 of the National Bank of Commerce maintained by TAC Traders Limited and 074103000100 of the National Bank of Commerce maintained by Daima Pharmaceuticals.

The money, the subject of the offence of money laundering as shown above originated from a theft that was earlier committed by one of the accused persons in the above case, namely, Justice Lemima Katiti, who was an accountant of the Tanzania Revenue Authority. The amount stolen as indicated in the charge sheet in Criminal Case No. 149 of 2010 was Tanzania Shillings one billion, four hundred twenty six million, four hundred fifty thousand, six hundred eighty and five cents (Tshs. 1,426,450,680.05). An interview with the presiding magistrate, revealed that the accused person used the electronic transfer systems to move the money from one account to others for the purpose of concealing its source.

Another case of the same nature that was referred to Kisutu Resident Magistrates'

Court in Dar es Salaam was the *Republic v. Faraji Augustino Chambo*.[114] In this case, Faraji Augustino Chambo was accused of two offences. The first one was obtaining money by false pretence contrary to sections 302 of the Penal Code, and the second was money laundering contrary to sections 3, 12(b) and 13(a) of the *Anti-Money Laundering Act*.[115] In the first offence, the particulars stated that the accused obtained by false pretence Tshs. 671,212,379.92 on the 30th day of June, 2008 in Dar es Salaam. The accused purported to show that the money was genuine payment from Tanzania Telecommunications Company Ltd to Trade Union Congress of Tanzania (TUCTA) for seminar activities.

After obtaining this amount of money, the accused moved the same from one account to another for the purpose of concealing its source. The accused had first transferred the amount from Account No. 011103001244 maintained by Tanzania Telecommunications Company Ltd at National Bank of Commerce, Corporate Branch to Account Number 01J1007892600 maintained by Trade Union Congress of Tanzania (TUCTA) and then transferred the same amount of money to Account Numbers 01J10028402800 maintained by Millennium Promotions Ltd at CRDB Bank, 018101006845 maintained by TUCTA at National Bank of Commerce, Mnazi Mmoja branch and 04710300144 maintained by Romos Technology Ltd at National Bank of Commerce. Immediately after transferring the above amount of money, the accused withdrew it from the mentioned accounts.[116]

[114] Criminal Case Number 168 of 2010.
[115] Act No. 12 of 2006.
[116] Another similar case is Criminal Case Number 146 of 2010 - Republic v. Marcus Mussa Masila and 5 others.

Another similar incidence took place in Arusha. In this incident, three accused persons, namely James Elineema,[117] Elineema James of Kitunda Engineering Co. Ltd., and Said Kakiva were charged before the Resident Magistrate's Court at Arusha, with conspiracy, forgery and stealing contrary to sections 384, 333, 335(a) and 337 and 265 of Penal Code. [118] The particulars of the offence of conspiracy indicated that the three accused persons did, on or about 5th day of January, 2009 at CRDB Bank Arusha Branch in Arusha, jointly and together conspire to commit the offences of forgery and stealing.[119]

The particulars of the second offence show that the three accused persons on the above mentioned date and place jointly and together forged an electronic bank transfer of CRDB purporting to show that the said Bank Transfer was genuine and valid while in fact it was not true. The particulars of the third offence detailed that the said accused persons did, at the above mentioned bank premises steal Tanzanian shillings amounting to 60,000,000/= via cheque number 675586, the property of CRDB Bank.[120]

Another incident occurred at NMB Bank in Manyara Region.[121] In this incident, six persons managed to unlawfully transfer Tshs.171, 000, 000/= Tanzanian Shillings

[117] James Elineema is a father to Elineema James. They are both directors of a company called Kitunda Engineering Co. Ltd.
[118] See Criminal Case Number 89 of 2009 at Arusha Resident Magistrate's Court. Records in respect of this file were accessed by the Researcher during the Field Survey.
[119] *Ibid.*
[120] *Ibid.*
[121] This incident was revealed to the Researcher during the Field Survey by Ms Naiman, the Head of Criminal Prosecution Department at the Office of the Attorney General in Tanga Region.

from a customer's account which was maintained in the same bank to their dubiously opened accounts in Chake Chake Pemba. Immediately, the same sums of money were transferred to another dubiously opened account held at NMB Madaraka Branch in Tanga. The criminals had purported to have been operators of an NGO called Ranifa Economic and Development Group and all documents used for registration of this NGO and later the opening of the mentioned account in Tanga were later found to have been forged.[122]

The criminals managed to withdraw Tshs. 58, 550, 000/= before the scam was detected. The only person who was arrested was one Khamisi Ally Salum, who sold building materials to those criminals. He was charged at Tanga Resident Magistrate's Court in connection with this offence and was later acquitted for lack of prosecution. Following this acquittal, the Office of the Attorney General in Tanga returned the file to the Regional Crimes Officer for further investigation, which may result in the arrest of the real culprits.[123]

The accused, namely Hassani Faraji @ Kimaro[124] was in the first instance charged before the Resident Magistrates' Court in Tanga with 274 counts of fraudulent false accounting contrary to section 317(b) of the Penal Code and 78 counts of stealing by servant contrary to sections 258 and 271 of the same Penal Code.[125] During the hearing, the prosecution alleged that the accused person with intent to defraud made false entries into the computer records in order to benefit himself from the

[122] *Ibid.*
[123] *Ibid.*
[124] See ***D.P.P v. Hassani Faraji @ Kimaro***, Criminal Appeal No. 30 of 2009, High Court of Tanzania, Tanga Registry (Unreported).
[125] *Ibid.*

difference in exchange rates of currency since 2002.

The accused person who was using the password ID.W 17 F, had been buying and selling USD at unapproved exchange rates. He posted in the system fictitious transactions that would reduce the balance of cash in records but the actual cash in his custody would not change. He would then pocket the difference and the actual cash would again tally with the balance of cash in records. As said above, the fictitious records started to be posted by the accused person from May 2002 to May 2003. He made several such false entries and each one made up an offence and a total number of entries rose to 353 automatically giving rise to the same number of counts.[126]

The amount of money that had been pocketed by the accused up to the time the fraudulent transactions were discovered was Tshs 434, 816, 650/=. The false records would show that there were purchases of United States Dollars at high rates and sold the same at lower rates. Two examples can be taken to illustrate how the fraud was committed. First, on 10th May 2003, the accused person made entries showing that USD 6800 was bought at the rate of Tsh. 1,120/= and sold at the rate of Tshs. 980/= each whereas the approved rates were Tshs. 1,015 and Tshs. 1038 for buying and selling respectively. It was this transaction that prompted investigation by the Internal Audit Department of CRDB at the Headquarters of the bank in Dar es Salaam.

[126] See Criminal Case Number 137of 2005 between the Republic and Hassan Faraji @ Kimaro. The records were accessed at the High Court, Tanga Registry during the field survey in Tanga on 20 June, 2013.

Second, on 15th January, 2003, the accused purported to have bought USD 38,000.00 at Tshs. 41,079,500/= using the rate of 1,067.00 instead of the approved rate of Tshs. 985 for each USD. Since the posting was a mere book entry as there was no actual purchase of dollars, his actual cash position remained the same as before posting this transaction but records showed that USD balance went up by 38,500 and Tshs. balance decreased to 41,079,500/=. After this fictitious purchase transaction, he posted another transaction but this was for sale of the same amount of dollars.

This transaction indicated that he sold USD 38,500.00 at Tshs. 36,190,000/=. The rate he used was 940 instead of 1,005. This was again a mere book posting because there was no actual receipt of and payment of cash and the actual cash position did not change. After this transaction, the cash records showed that he paid out USD 38,500.00, the amount he bought in the previous transaction and received Tshs. 36,190,000/=. The USD balance was, therefore, reduced by 38,500.00 and Tshs. balance was increased by 36,190,000/=. The net effect of the two transactions as reflected in the cash records is that there would be no change of USD balance whereas the Tshs balance would decrease by 4,88,500, i.e, 41,079, 500/= minus 36,190,000/=.

Regarding the operation of the computer system, the court was told that the bank operations were entered and stored in particular soft-ware systems which had a Banks Master as the central server for all CRDB bank transactions country-wide. Each branch of the bank had a network that linked cashiers/tellers and their

supervisors, super-users, branch controller and branch manager. Each branch had also a server called Branch Power which was capable of storing record/report for some time and the main server (Bank Master) received the record sent from the Branch Power.

In order to be able to work using the system, each staff of the bank had his/her password that identified him. It was this password that authorized a staff to operate transactions in the system and that the password was confidential. It could not be altered or changed without the awareness of the user. There were different levels and limits in using the system. The limit for the accused person was 5,000,000/=. However, as facts show above, he exceeded this limit without being authorized.

The procedure for purchasing foreign exchange (forex) was that a customer had to see the Departmental Manager or the customer advisor with relevant documents. When the departmental manager or the customer advisor was satisfied, he/she forwarded the forex request amount requested to the cashier/teller. The cashier/teller fed the system with the data and forwarded the same to the supervisor /departmental manager and then to the Branch Manager for authorization and approval of the transaction. When the transaction was approved, the vouchers were then printed but where there was no such approval the transaction could not be completed in the system. In the event the cashier/teller fed the system with a wrong rate of forex, the Branch Power would reject it by displaying the message “Invalid Exchange Rate”. The rate was centrally controlled by the Bank Master and could not be altered by the Teller.

The question before the court was how was it possible for the invalid exchange rates to be accepted by the Bank Master without sending back the message to the users/management? The computer expert from the headquarters told the court that the record was electronically received by the Bank Master when the system was offline. The defense contended that the computer system could not work properly while it was offline. Were the computer system online, the fraudulent transactions would not be made because the system operator at the headquarters could have discovered the same. The prosecution alleged that the fraudulent transactions were made during the time when the system was offline. During this time when the system was off-line, the transactions by- pass the branch power or server and are communicated directly to the main server at the headquarters, leaving the branch manager without any means to verify and authorize transactions.

It was stated in court that the fraudulent transactions should have been discovered by the branch supervisor who was supposed to approve transactions operated by the accused person. However, it was pointed out that the supervisor colluded with the accused person by giving him rights to edit entries in the computer system. Each transaction required vouchers and investigation revealed that the accused had no vouchers to support the transactions and that the false entries could not be discovered because the accused deleted the entries in the system before the supervisor printed the daily reports.

In his defense, the accused told the trial court that the procedure when a client buys foreign currency from the bank is that the customer has to see the customer adviser who, if satisfied that the client meets the laid down requirements, receives and

forwards the supporting documents to the departmental manager for approval. Where the teller does not have enough amount of foreign exchange needed by any customer, he issues a treasury out-slip requesting for extra currency from the strong room. The amount has to be recorded in the cash amount register. The sale transaction is then posted to the computer and referred to the departmental manager for approval before the Teller's account is debited. It is after this step that the voucher is printed and the client signs the same. The teller also signs and issues one copy to the client while the bank retains the other. The accused told the court that it was not possible for him to vary the exchange rate because the computer system would reject and indicate "invalid exchange rate".

Acquitting the accused, the Resident Magistrate based his reasoning on doubts in the operation of the system. The fact that the supervisor had access to the accused person's computer made the magistrate doubt whether the false entries were made by the accused or the supervisor. The relevant section of the judgment reads as follows:

> *"I, however, hasten to point out that in the system of maintenance, the super-user and branch manager have the facility to break and change the cashier/teller passwords. Furthermore, as it is conceded that the super-user had capacity of controlling end of the day reports and authorizing transaction, I am inclined to believe that the super user and branch manager smoke screed the fraudulent transaction in the user ID and cash amount of the accused."*

Furthermore, the fact that the computer should have been operated while it is online

cast doubts whether the entries were actually made. For purpose of clarity a section of the judgment to this effect reads as follows: The super user had the gigantic powers over transactions. I don't think if the branch overshadowed on the fact that those powers could have the negative effects on transactions.

PW.4 has contended that it was possible to post the transaction while the system was offline. It is surprising, this contention does not appear in the audit/investigation report (Exh.P90). It was not specifically explained as to when and what caused the system to be offline. Albeit, I am not a computer software technician, I understand that whenever the system is offline there cannot be dissipation of transaction. But, when online the exchange rate cannot be tempered with otherwise it will indicate the word "invalid exchange rate" and instantly will forward the same as referral to the supervisor or super user who could authorize the same.

The doubt that the trial magistrate had was how could the rates that had not been approved pass through the system? In other words, how could the accused person exceed his limit? The trial magistrate formed an opinion that This case was a fit one for conspiracy, so to say. The prosecution side will agree with me in that the accused in his position as a cashier/teller couldn't interfere with the exchange rate restriction system unless otherwise there was cooperation with other senior Bank officials. In absence of the evidence of conspiracy, this creates a lacuna in prosecution case, which, in reality is fundamental in that it goes deep to the roots of prosecution case.

Based on the reasons above, the trial magistrate acquitted the accused person for lack of sufficient evidence to prove the charges of fraudulent false accounting and stealing by servant. The Republic, aggrieved with the decision by the trial court, appealed to the High Court of Tanzania, Tanga Registry. One of the grounds of appeal was that the trial magistrate erred in fact and law in holding that the fraudulent transactions could not pass through the Bank Computer system while the system was offline. Arguing this ground of appeal, the state attorney in his submissions told the High Court Judge who heard the appeal that the evidence of a computer expert PW 4 one Ambwene Andrea was clear that the computer system could work offline and allow invalid exchange rates to pass through the system.

The High Court Judge posed the question as to how the computer system could allow the invalid rates to pass on without sending the message to supervisors. The learned judge was, however, convinced with the expert witness to the effect that it was possible for the main server to have records directly from the branch server in it despite the system being offline. What she doubted was the fact that all the fraudulent entries were made during the days when the system was offline. However, the Judge formed an opinion that the accused had conspired with one of his supervisors, who was a super-user at the Branch namely Tryphone Muchunguzi. According to the Judge, Muchunguzi was in control of the Branch Power and was charged with printing daily reports and he must have concealed the fraudulent transactions made by the accused.

On powers of the super-users, supervisors and bank managers, the Judge was of the

view that despite the fact that the same can inquire, post static data, authorize referrals, change passwords, currency refresh and remove lock out flags, the evidence shows that they cannot do so without the knowledge of the users. At the end, the passwords remain a secret to the user.

The Judge formed a further opinion that the accused person had admitted tempering with the exchange rates in the computer system and when a transaction he posted on 10th May, 2003 was discovered, he reversed the same to reflect the correct rates. The relevant part of the High Court Judgment reads as follows: This is contained in Exh. P. E. 88 where the respondent reversed the Teller log to record the correct authorized rates in respect of 10/5/2003. The respondent reversed the entries on 15/5/2003 to reflect the correct rates of Tshs.1015/= @ USD for buying and shs. 1038/= USD for selling. Initially, the respondent had posted figures showing that the rates were shs. 1,120/= for buying and shs.980/= for selling as they were on 10/5/2003.

Based on the above facts, the Judge concluded as follows: In my considered view, this is an evidence that the respondent fed the computer system with wrong entries/exchange rates. Again it is on evidence that by using the un-authorized exchange rate, there was a difference of 940,000/=. This amount was alleged to have been stolen from that transaction. PW. 1 testified to the trial court that having discovered the fraud in the transaction, and the respondent having admitted, the latter also admitted that he was ready to pay the difference.

On conspiracy, the Judge found as follows:

The record shows that the prosecution testified that the respondent managed to defraud the bank only when the late Tryphone Muchunguzi was on duty. The evidence is to the effect that when any of the two were on leave no such fraud was detected in the branch transactions. If the password was confidential to an individual, then the data reflecting the ID.No. W.17.F could not be processed and sent in the absence of the respondent even if Muchunguzi the super-user, was on duty.

Likewise, when Muchunguzi was on duty no fraud was reported or detected from W.17.F as the user was not active in his account. All these facts taken together, they lead to the proof and conclusion that the two had conspired to commit the fraudulent accounting in the bank. Allowing the appeal and convicting the accused, the Judge said:

> *"I am therefore convinced by the evidence on record that the prosecution managed to prove beyond doubt the offences of fraudulent false accounting in counts Nos: 346, 347, 348 and 349 and stealing by servant in count No.350".*

The appeal is therefore allowed to this extent only. The acquittal in respect of these counts is set aside and replaced by a conviction. The respondent is therefore convicted accordingly.

Following the above decision by the High Court, the defense has lodged an appeal to the Court appeal, which is pending to date. Despite the fact that the appeal has not yet been determined, this decision of the High Court may be criticized on a

number of grounds. First, an analysis of the law that was used to charge the accused was not made. The question that the court ought to have asked itself was whether the offence of stealing could be committed when the evidence showed that it was only data that had been manipulated.

Even if the end result of the transaction was to benefit the accused in terms of monetary value, yet the elements that constitute the offence of stealing should have been discussed and a determination whether the elements existed in the case before the court ought to have been made. Second, the procedure for authentication and authorization of banking transactions in electronic form should have been given a judicial pronouncement.

In the case before the court, the use of passwords as a method of authenticating transactions was in issue. The question would be: was the use of passwords authorized by law? This question was relevant because there was a contention by the defense that the super user could as well access the accused person's password and effect any changes. The third question is in relation to admissibility of computer generated evidence. The use of e-banking technologies, as said earlier in this Study, dispenses with the use of paper. Data messages or electronically generated documents have now found way to courts of law to prove or disprove a fact in issue. The high court ought to have made a determination whether the evidence generated by computers or electronic bank records were admissible and if admissible, how would security, authentication and reliability be determined. These issues were left for determination, perhaps by the Court of Appeal when hearing the appeal arising

from this decision.

The relevance of bringing these incidents to light which led to massive losses of both banks' and customers' money is three fold. First, in order for electronic funds transfer involving huge amounts of money to be successful, there must in most cases be an involvement of an employee of the bank. Second, the customers' monies in banks are not safe due to the presence of unfaithful employees, who have access to customers' accounts information. Third, bank customers may conspire with employees of the banks in order to allow crime to be perpetrated using their accounts.

2.4 Conclusion

The aim of this chapter was to lay a conceptual framework for electronic banking. It defined e-crime and identified a few incidents of cyber crimes at the international level, the purpose being to lay a foundation for recommendations of a suitable legal framework in Tanzania.

CHAPTER THREE

3.0 LEGAL FRAMEWORK ON CYBER CRIME

3.1 Introduction

The purpose of this Chapter is to present a discussion on how the penal laws address the cyber crimes in Tanzania. It will show that the existing legal framework on criminal law has no such offences referred to as cyber crimes. It is doubtful whether the existing principles on criminal law designed to regulate paper –based transactions can apply to theft and frauds in electronic banking. However, this point is being increasingly recognized as an area of concern and more and more countries are, therefore, enacting specific and comprehensive legislation to cover the acts of computer criminals.

3.2. Cyber Crime Legislation in Africa

The East Africa region includes Tanzania, Kenya and Uganda, while the Southern African Development Community (SADC) region includes Zambia, Zimbabwe, South Africa, Malawiand Mozambique. The SADC region started harmonizing cyber crime laws in 2006 to deal with cross-border criminals. The new laws allow member countries to prosecute cybercriminals despite where the crime was committed in the SADC region.

However, progress has been slow in several countries, such as: Kenya and Uganda who have not proposed draft laws to their respective parliaments. Mauritius, South Africa and Zambia have adopted cyber crime legislation. Botswana finally has a cyber crime law, passed by Parliament in December 2007 and signed into law by

President Festus Mogae later in the same month.127

3.3 Legal Framework on Cybercrimes in Tanzania

As pointed out above, persons who used mobile phones and ATM cards to transfer money from other persons' accounts in Tanzania have been charged with the offence of theft contrary to section 265 of the Penal Code, Cap. 16. This provision reads as follows:

> *"Any person who steals anything capable of being stolen is guilty of theft, and is liable, unless owing to the circumstances of the theft or the nature of the thing stolen, some other punishment is provided, to imprisonment for seven years."*

It appears that the above section does not create the offence of theft; it rather provides punishment for the offence. The provisions that create the offence of theft are sections 257 and 258. Section 258 defines the offence of theft while section 257 stipulates things that are capable of being stolen. The elements of the offence of theft according to section 258 consist of anything capable of being stolen, act of appropriation, a certain type of property, unlawfulness and intention, including an intention to appropriate.

The *actus reus* of the offence of theft is aspiration, which is referred to as the physical handling of the thing or property. This property or thing must be capable

---

[127] Masadeh, A. M. S, Combatting Cyber crime: Legislative Approach: A comperative analysis between Quatar, UK and UAE, accessed at http://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en

of being stolen.[128] The obvious requirements that the thing must meet before being capable of being stolen are that it must be movable, it must be corporeal and it must belong to someone else.[129]

From the elements of the offence of theft only tangible things that are capable of being moved from one place to another may be stolen. That being the case, it is questionable whether or not theft may be committed in e-banking transactions. As stated earlier in Chapter Two of this study, computers are currently used to process, store and disseminate data involving monetary value. When a person accesses a computer or an intelligent device, he has a number of motives, one being to transfer money. At that time he is moving data with monetary value and later he accesses money using an ATM machine. It is doubtful whether information or data could qualify as a subject of theft. This is a *lacuna* in the legal system in Tanzania. It is argued in this study that the law must define the term 'property' or 'thing' to include incorporeal property or thing in order to render data or information capable of being stolen.

The closest offences in relation to computer data theft are unauthorized access to the computer and unauthorized access with ulterior intent. The Malaysian experience as discussed in Chapter Three provides a clear guidance on how these offences may be related to the offence of theft in the Penal Code. In Malaysia section 3(1) of the Computer Crimes Act 1997 creates an offence of unauthorized access and section 4 (1) and (2) of the Act creates an offence of unauthorized access with ulterior intent.

[128] See section 257 of the Penal Code Act, Cap. 16.
[129] *Ibid.*

It is this law that provides for a legal basis to punish a person who secures the unauthorized access to a bank's computer in order to divert funds into his bank account maintained in another bank. It also punishes a person who secures the unauthorized access to a bank's computer and instructs the bank's computer to round down the interest calculated on all interest-bearing accounts, and the excess funds diverted to his/her personal account.

It is argued in this study that without laying a clear basis for punishment of crimes in relation to computers and other intelligent devices used by banks to store monetary values, any claim that one has used a mobile phone or an ATM card to steal or transfer money may lack any legal basis.

As also observed above, suspects of e-crimes in Tanzania are also charged with the offence of forgery contrary to sections 333, 335(a) and (d), (i) and 338 of the Penal Code, Cap 16. Forgery in banks can take a number of forms. First, a person forges a transfer statement that authorizes movement of funds from one account to another. The form in this respect is paper-based, but the actual transfer is done electronically, different to when a cheque is involved. Once the form is accepted by the bank the transfer becomes instantaneous and it cannot be reversed.

The second type of forgery is when a person counterfeits someone's plastic card and uses it to withdraw funds from the account belonging to that person. For access to the account to be possible, the thief or fraudster must have knowledge of the person's PIN or Code. The third is when a person sends electronic instructions to authorize transfer of funds whereas he has no such authority to do so. For example,

a person may send an email to the bank instructing it to transfer funds from one account to another. A good example is the officer of the Tanzania Revenue Authority who purported to be an accountant of the Tanzania Telecommunication Company and instructed the NBC bank to transfer millions of money to various accounts held in a number of banks.[130]

Section 333 of the Penal Code defines the offence of forgery as the "making of a false document with intent to defraud or to deceive." From the provision of section 335 of this law, a person would be guilty of the offence of forgery if he

(i) Makes a document which is false or which he has reason to believe is untrue;

(ii) Alters a document without authority in such a manner that if the alteration had been authorized it would have altered the effect of the document;

(iii) Introduces into a document without authority, whilst it is being drawn up, matter which if it had been authorized would have altered the effect of the document;

(iv) Signs a document–

(v) In the name of any person without his authority, whether such name is or is not the same as that of the person signing;

(vi) In the name of any fictitious person alleged to exist whether the fictitious person is or is not alleged to be of the same name as the person signing;

[130] See Criminal Case No. 146 of 2010 *the Republic v Marcus Mussa Masila and 5 others* (The case is still pending at Kisutu Resident Magistrates' Court of Dar es Salaam.

(vii) In the name represented as being the name of a different person from that of the person signing it and intended to be mistaken for the name of that person;

(viii) In the name of a person personated by the person signing the document, provided that the effect of the instrument depends upon the identity between the person signing the document and the person whom he professes to be.

From the provisions of the law in relation to forgery as pointed out above, it is arguable whether criminals who transferred funds using electronic messages that have been forged or cards that have been counterfeited can be brought to justice. The above provisions relate to forgery of documents and it is certain under the current law that a document does not include an electronic message, data or document. It is argued in this study that the Penal Code Act needs to be amended to clarify this aspect, particularly when new technologies make it possible for the offence of fraud to be committed using computers and computer networks. The issue that haunts the court is whether computer fraud amounts to forgery.

As indicated above, the offence of money laundering is charged under sections 3, 12(b) and 13 (a) of the Anti-Money Laundering Act, No. 12 of 2006. Sections 12(b) creates the offence of money laundering in the following words

12. *A person who –*

(a) …

(b) Converts, transfers, transports or transmits property while he knows or ought to know or ought to have known that such property is

> *the proceeds of a predicate offence, for the purpose of concealing, disguising the illicit origin of the property or of assisting any person who is involved in the commission of such offence to evade the legal consequences of his actions.*
>
> *(c) . . .*
>
> *(d). . .*
>
> *(e). . .*

A list of predicate offences is given under section 3 of the Act, some of which are illicit drugs trafficking, terrorism, illicit arms trafficking, corrupt practices, counterfeiting, armed robbery, theft, forgery, tax evasion, illegal mining and environmental crimes. A person who is guilty of the offence of money laundering shall be sentenced to a fine not exceeding five hundred million shillings and not less than one hundred million shillings or to a term of imprisonment not exceeding ten years and not less than five years.[131] There is no mention of electronic crimes in the list and one wonders why the omission despite the Act being enacted in 2006 when ICT had already gained a very important place in the operations of banking business.

As seen above, the culprits transfer money electronically from one account to another with ease, instantaneously and without the ability to trace it. It is doubtful whether the interpretation of the term "transfer" includes an electronic transfer. This doubt is justified by the fact that the Act makes no mention of electronic transfer. Indeed, it does not even define the term 'transfer'.

[131] See section 12 of the Anti-Money Laundering Act of 2006.

Where the offence of money laundering has been committed, section 65B of the Proceeds of Crime Act empowers a police officer above the rank of Superintendent to have access to computer data in order to obtain evidence in relation to commission of the crime of money laundering. This nature of evidence seems to be admissible under the new amendment to the Evidence Act of 1967 as discussed above. The challenges revolving around this kind of evidence, generated by computers, are reliability, security and authenticity.

Section 116 of the Electronic and Portal communication run as follows:

i. Any person who installs, operates, constructs, maintains, owns or makes available network facilities without obtaining any relevant individual license, commits an offence and shall be liable upon conviction to a fine of not less than five million Tanzanian shillings or imprisonment for a term not less than twelve months or to both.

ii. Any person who provides network services without obtaining any relevant individual license, commits an offence and shall be liable upon conviction to a fine of not less than six million Tanzanian shillings or imprisonment for a term not less than twelve months or to both.

iii. Any person who –

(a) Provides application services without having first obtained any relevant individual license;

(b) Provides content services without having first obtained any relevant individual license, or any relevant class license commits an offence and shall be liable upon conviction to a fine of not less than five million

Tanzanian shillings or imprisonment for a term not less than twelve months or to both;

(c) Imports, distributes, or sells electronic communication equipment or apparatus or; establishes, installs, maintains and operates an electronic communication system or imports non type approved electronic communication equipment or apparatus into the United Republic without a license, commits an offence and shall be liable upon conviction to a fine of not less than five million Tanzanian shillings or imprisonment for a term not less than twelve months or to both.

Section 118 of the Electronic and Postal Communication Act[132] makes an offence to create obscene communication like child pornography and other offence of such nature. Section 118 of the same Act run as hereunder,

Any person who-

i. By means of any network facilities, network services, applications services or content services, knowingly makes, creates, or solicits or initiates the transmission of any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person;

ii. Initiates a communication using any applications services, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threatens or harass any person at any number or electronic

[132] ibid

address;

By means of any network services or applications service provides any obscene communication to any person; or

iii. Permits any network services or application services under the person's control to be used for an activity described in section 117 (3),commits an offence and shall, on conviction, be liable to a fine not less than five million Tanzanian shillings or to imprisonment for a term not less than twelve months, or to both and shall also be liable to fine of seven hundred and fifty thousand Tanzanian shillings for every day during which the offence is continued after conviction.

iv. Section 120 of the Electronic and Postal Communication Act[133] creates a penalty for interception of communication and it provides that: Any person who, without lawful authority under this Act or any other written law-

Penalty for interception of communications

(a) Intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept any communications; or

(b) Discloses, or attempts to disclose to any other person the contents of any communications, knowingly or having reason to believe that the information was obtained through the interception of any communications in contravention of this section; or

(c) uses, or attempts to use the contents of any communications, knowingly having reason to believe that the information was obtained through the interception of any communications in

[133] ibid

> contravention of this section, commits an offence and shall, on conviction, be liable to a fine of not less than five million Tanzanian shillings or to imprisonment for a term not less than twelve months, or to both.

Under that Section 120[134] the penalty is imposed if there is date interception the penalty inflicted is Tshs 5,000,000 or 12 months imprisonment or both fine and imprisonment. Here punishment as compared with International Law is left to the member state, the Convention never intend to punish criminals but creates only the offence under the cyberspace. Jurisdiction under the cyberspace is left to the member state after creating its own cyber law and other procedural law or rules.

Section 122[135] deals with fraud with dishonest intent while Section 124[136] deals with illegal access to computer system like in the Budapest Convention. Section 123[137] inflicts penalty to a person for interference of electronic communication to be a fine of not less than Tshs 5 million or 2 years imprisonment or both fine and punishment. This is not the case to the Convention. If we can consider the Indian domestic law particular Section 43 of the *Information Technology Act*[138]. Which is national law of India creates a penalty like our law for damages for the computer and computer system. The criminal is liable to pay damages by way of compensation for the sum not exceeding 1 crone rupees to the victim. Section 43 provides as hereunder: If any person without permission of the owner or any other

[134] Supra
[135] Supra
[136] ibid
[137] Supra
[138] Act No.21 of 2000

person who is in-charge of a computer, computer system or computer network,

i. Accesses or secures access to such computer, computer system or computer network;

ii. Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

iii. Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

iv. Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

v. Disrupts or causes disruption of any computer, computer system or computer network;

vi. Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

vii. Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there-under;

viii. Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

As Mwiburi,[139] pointed out, cybercrimes are intermingled with electronic commerce like e- signature, digital signature, digital devices and e-contracts and that they ought to have been addressed because they are very important. It is argued here that the legal regime in Tanzania in respect of cyber crimes is still wanting and that EPOCA has not addressed all the issues in respect of cyber crimes, hence, inadequate because it leaves a big lacuna in the legal regime on cybercrimes.

3.4 Conclusion

As observed above, detailed rules exist in relation to theft and frauds in paper -based transactions. It is noted that computer crime detection are a difficult task. Bringing the criminals to book becomes a formidable challenge since the laws in many countries have not kept pace with technology. Laws were originally designed to protect tangible assets and may not be sufficient to guarantee the protection of electronic bits of data. It is often difficult to attribute guilt using the existing statutes since the act of trespassing into a system and tampering with virtual data may not necessarily be specifically provided for in law.

[139] Mwiburi, A.J., op.cit.

CHAPTER FOUR

4.0 LESSONS FROM OTHER JURISDICTIONS

4.1 Introduction

As noted in Chapter Two of this Work, criminals use computers and computer networks to perpetuate their ill motives like accessing customers' accounts and making fraudulent transfers. In most incidents, huge losses are caused by this unauthorized access either to banks or customers. It is this problem that Bainbridge regards as having spurred on legislative activity to create new criminal laws or to strengthen existing ones.[140] This Chapter will analyse how other jurisdictions have addressed cyber crimes by use of legislation

4.2The need for Legislation on Cyber Crimes

The world first computer specific law was enacted in the year 1970 by the German State of Hesse in the form of *'Data Protection Act,* 1970' with the advancement of cyber technology. With the emergence of technology the misuse of technology has also expanded to its optimum level and then there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect technological advancement system.[141]

4.3 The Position in Malaysia

In Malaysia, *the Computer Crimes Act* 1997 provides for offences relating to the misuse of computers. The Act makes it an offence if there is an unauthorized access to computer systems and the use of computer systems for fraudulent purposes. The

[140] Bridge, B., *op.cit*., p. 5.
[141] See http://www.legalindia.in/cyber-crimes-and-the-law

Act also provides that the commission of these offences extraterritorially (that is, outside Malaysia) is punishable. Section 9(1) of the *Computer Crimes Act* 1997 states that the provisions of this Act shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia.

Section 2 of the Act defines the word 'computer' as an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility.

> "*Computer network" means The interconnection of communication lines and circuits with a computer or a complex consisting of two or more interconnected computers*".

Section 2(10) of the Act provides further that "any reference in this Act to a computer includes a reference to a computer network. The Computer Crimes Act 1997 defines "data" as "representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer". And, the

word “program” means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

Section 3(1) of *the Computer Crimes Act* 1997 creates an offence of unauthorized access. It provides that a person shall be guilty of an offence if: (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorized; and (c) he knows at the time when he causes the computer to perform the function that that is the case.

Section 3(2) of the Act provides that

> *“The intent a person has to have to commit an offence under this section need not be directed at: (a) any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer”*

The Computer Crimes Act 1997 defines the scope and meaning of “unauthorized access” in section 2(2) and (5). The burden of proof on the prosecution is made easier by section 8 of the Act, which provides: A person who has in his custody or control any program, data or other information which is held in any computer or retrieved from any computer which he is not authorized to have in his custody or control shall be deemed to have obtained unauthorized access to such program, data or information unless the contrary is proven. Therefore, once it is proven that the accused has custody or control of the program, data or other information and that he or she was not duly authorized, the accused has to prove otherwise.

Thus, what constitutes "custody or control" is important. The learned Gunn Chit Tuan J. (as he then was) in *Public Prosecutor v Ang Boon Foo*[142] held that control must connote something more than mere knowledge of the thing in question. That something is an element of dominion over the material. It must be shown that the person who had knowledge of its whereabouts had also access to it and could at any opportune moment of his choice have obtained possession of it or the capacity to direct its disposal. The Court here referred to the Australian case, *Johnston Fear and Kingham v Commonwealth,*[143]which held that the word "control" is "wide enough to include many types of possession which are not commensurate with full ownership".

The Court also made reference to the English case, *Dolfus Mieg Er Compagnie SA v Bank of England,*[144] which held that "control" would cover the right to tell the possessor what is to be done with the property. On the other hand, the word "custody" appears to require an element of care or guardianship. In the Singapore case of *Ho Seng Seng v Rex,*[145] Brown Ag CJ held: "I would adopt the following definitions of "custody" and "possession" given by the eminent American jurist, Roscoe Pound, in his *Introduction to American Law*:

Custody is a mere condition of fact, a mere physical holding of or physical control over the thing. Where custody (exercised by oneself or by another) is coupled with the mental element of holding for one's own purpose, there is possession." The

[142] [1981] 1 MLJ 40 at p.42.
[143] 67 CLR 314
[144] [1950] Ch. 333.
[145] [1951] MLJ 225

above passage was cited in *Neo Koon Cheo v Reg*[146] by Ambrose J. In *Public Prosecutor v Ang Boon Foo*[147] Gunn Chit Tuan J (as he then was) made the following distinction between the words "custody" and "possession": "The main distinction between custody and possession is that a custodian has not the power of disposal. The statement that "possession must be exclusive" is often due to confusion of the fact to be proved, with the evidence by which it is to be proved. It is essential to keep this distinction clearly in mind, especially when applying presumptions."

In other words, a person is said to have custody over an article if he has de facto possession of it or has care over it. Thus, a person is said to have "control" over a program, data or other information if he knows of its existence and has dominion over the person in whose possession the program, data or information is found. And, a person is said to have "custody" if the factual situation points to the accused exercising some care over the item.

The prosecution must prove either the element of "custody" or "control" since section 3 uses the word "or". If neither element is proven then the presumption in section 8, as stated above, will not apply. The maximum sentence, stipulated in section 3(3), *Computer Crimes Act* 1997 which a court may impose under this section is a term of imprisonment not exceeding 5 years or a fine of up to RM50,000.00 or both such a fine and imprisonment.

---

[146] [1959] MLJ 47.
[147] [1981] 1 MLJ 40.

Section 4 (1) and (2) of the Computer Crimes Act 1997 creates an offence of unauthorised access with ulterior Intent. It states that "(1) A person shall be guilty of an offence under this section if he commits an offence referred to in section 3 with intent –(a) to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code; or (b) to facilitate the commission of such an offence whether by himself or by any other person.

Thus, the offence, which this section creates, is limited to those offences which involve fraud or dishonesty or which cause injury as defined in the Penal Code.[148] Examples of section 4(1)(a) offences are: (1) A person secures the unauthorized access to a bank's computer in order to divert funds into his bank account maintained in another bank; or (2) A person secures the unauthorized access to a bank's computer and instructs the bank's computer to round down the interest calculated on all interest-bearing accounts, and the excess funds of half seen be diverted to his personal account; Such person can be said to have committed theft under the Penal Code and would have committed offences under both sections 3 (for the unauthorized access) and 4 of the *Computer Crimes Act* 1997.

Section 4(1)(b) requires the person securing access "to facilitate the commission of such an offence whether by himself or by any other person". Section 4(3) provides that a person guilty of the section 4 offence shall on conviction be liable to a fine not exceeding RM150,000.00 or to imprisonment of up to 10 years or to both.

[148] See Chapter XVIII and sections 206-210, 415, 421-424 and 474, Penal Code for offences involving fraud; sections 209 and 378-424, Penal Code for offences on dishonesty; and Chapter XVI of the Penal Code for offences causing injury.

Section 5(1) creates the offence of unauthorized modification of contents of computer. It renders it an offence if a person who does "any act which he knows will cause unauthorized modification of the contents of any computer." An essential element of this offence is knowledge. In the case of *Lai Fook Kee v Public Prosecutor*[149] the court relied on two authorities for the definition of the word "knows" and stated thus: "In *London Computator Ltd v Seymour*[150] it was held that the word "knows" bears its ordinary meaning and is not so to be construed as "ought to have known". In *Sinniah Sokkan v Public Prosecutor*,[151]

Gill J (as he then was) was considering the meaning of "knowingly made a false statement" and he stated: "… it must not only be proved that the statement was false but also that it was conscientiously made and known to be false". In the absence of specific finding … of personal knowledge by the appellant that the statement which he gave was false, the conviction cannot stand and the appellant must be acquitted."

Besides having to prove that the accused had personal knowledge that the access was unauthorized, it must also be proved that there was an "act". Thus, examples of acts, which may constitute offences under this section, include: (1) deliberately closing of a word processing program without saving the changes made to the information by moving the mouse or by switching off the power supply; (2) introducing a "worm" program into the computer system so that by adding programs or data to the computer's content, all the spare capacity in the computer is

[149] [1970] 1 MLJ 134
[150] [1944] 2 All ER 11
[151] [1963] MLJ 249

used up; and (3) intentionally introducing a computer "virus" into the system.

Subsections 5(2) and (3) of the *Computer Crimes Act* 1997 go on to provide: "(2) For the purposes of this section, it is immaterial that the act in question is not directed at – (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer. (3) For the purposes of this section, it is immaterial whether an unauthorized modification is, or is intended to be, permanent or merely temporary."

Section 2(7) explains what "modification" in this context means: "[A] modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer – (a) any program or data held in the computer concerned is altered or erased; (b) any program or data is introduced or added to its contents; or (c) any event occurs which impairs the normal operation of any computer, and any act that contributes towards causing such a modification shall be regarded as causing it."

Thus, a modification occurs where a function[152] of the "target" computer itself is operated. Subsection 2(8) goes on to provide that such modification is "unauthorized" if: "(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and (b) he does not have consent to the modification from any person who is so entitled."

[152] A "function" is defined in section 2(1) as including "logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer".

Section 5(3) provides that it is immaterial whether an unauthorized modification is, or is intended to be, permanent or merely temporary. The section would catch mere transient forays into another computer's system if there were an unauthorized modification. A person guilty of a section 5 offence shall on conviction be liable to a fine not exceeding RM100,000.00 or to imprisonment for a term of up to 7 years or to both. The penalty is enhanced, to a maximum fine of RM150,000.00 or maximum imprisonment of 10 years or to both, if the act is done with the intention of causing injury as defined in the Penal Code.[153]

Section 6 creates the offence unauthorized communication of codes or passwords. It makes it an offence to communicate directly or indirectly a number, code, password or other means of access to a computer to any unauthorized person. A person guilty of this offence shall on conviction be liable to a maximum fine of RM25,000.00 or to imprisonment for a term of up to 3 years or to both.

As the marginal note of this section and the Explanatory Notes to the *Computer Crimes Act* 1997 use the words "wrongful communications", it is submitted that an offence under section 6 cannot be committed by inadvertence. Means area (intention) is necessary to make it an offence to wrongfully communicate the number, code, password, etc. to an unauthorized third party.

The other element to be proven is the information given (in the form of a number, code, password or other means) has the effect of enabling the third person (who is

[153] Section 5(4), Computer Crimes Act 1997.

unauthorized to do so) to gain access to a computer. Bankers, in particular, should take heed of this section as the scope of this provision is very wide and would cover situations where their passwords or access codes are communicated to their colleagues who are not authorized such access.

In relation to powers of law enforcement agencies, under section 10(1) of the *Computer Crimes Act* 1997, the powers of the law enforcement agency to search and seize evidence are subject to a warrant to be issued by the Magistrate. The Magistrate must have reasonable grounds for believing that the commission of an offence is committed.[154] The Magistrate must have sufficient facts to form the basis of his belief.

The powers given to the police under section 10(2) of the Computer Crimes Act 1997 are very wide. The section provides: "(2) Whenever it appears to any police officer of or above the rank of Inspector that there is reasonable cause to believe that in any premises there is concealed or deposited any evidence of the commission of an offence under this Act, and the police officer has reasonable grounds for believing that by reason of the delay in obtaining a search warrant the object of the search is likely to be frustrated, he may exercise in and in respect of the premises all the powers mentioned in subsection (1) in as full and ample a measure as if he were empowered to do so by warrant issued under that subsection.

Under the Act, any police officer may arrest without a warrant any person whom he reasonably believes to have committed or to be committing an offence against this

[154] See In re Kah Wai Video (Ipoh) Sdn. Bhd. [1987] 2 MLJ 459 at p.461 per J. Edgar Joseph Jr.

Act, and every offence against this Act shall be deemed to be seizable offence for the purposes of the law for the time being in force relating to criminal procedure." Thus, under certain circumstances and conditions, the police may search without a search warrant and arrest without a warrant.

Under section 11, a person guilty of the offence of obstructing a search shall on conviction be liable to a maximum fine of RM25,000.00 or to imprisonment of up to 3 years or to both. Section 12 of the Computer Crimes Act 1997 provides that all prosecutions under the Act can only be instituted by or with the written consent of the Public Prosecutor.

4.4 Position in the US

In the US, the *Computer Fraud and Abuse Act* creates a number of offences, including the offence of unauthorized access to computers.[155] It seeks to punish many of the activities commonly referred to as hacking.[156] Under this law, it is illegal to have access without authorization to any computer system to obtain financial information held by any financial institution, credit information held by a consumer reporting agency, or credit card information held by the issuer of credit cards.[157]

4.5 Position in India

Cyber crimes in India have seen a sudden spurt. Cyber crimes have gone up by 60 per cent in 2012 at 3,500 as against 2,070 in the previous year. The figures collected

[155] See Cavazos, E & Morin, G., Cyber Space and the Law: Your Rights and Duties in the On-Line World, 4th Edition, The MIT Press, London, 1996, p. 107.
[156] *Ibid.*
[157] See section 1030 of the Computer Fraud and Abuse Act.

by National Crime Records Bureau (NCRB) give a graphic description of how cyber crimes have spread across the country. Maharashtra topped the list with 561 (393 in 2011) crimes, followed by Andhra Pradesh with 454 (372) and Karnataka 437 (160).[158]

The data found that majority of the crimes are being done by criminals in the age group of 18 to 30. "Financial offences dominate cyber crimes. Of late, we have noticed an increase where the fraudsters hacking into email accounts of companies and of customers. They read the entire email thread and lure the customers to deposit money in a fake account, duping both," T.S. Uma Maheswara Rao, Inspector of Police (Cyber Crime Police Station, Hyderabad), told *Business Line*.

The aggregate losses suffered by customers and companies in the last one year in Hyderabad were put at Rs 2 crore. The NCRB, which monitors and records crimes of all sorts across the country, has compiled a detailed cyber crime scene in the country, giving a break-up of cases under the IT Act and the Indian Penal Code. The list includes a variety of crimes – disgruntled employees breaking into systems, eve-teasing, revenge, extortion and financial crimes.

There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the

[158] See http://www.thehindubusinessline.com/industry-and-economy/info-tech/financial-offences-top-cyber-crimes-in-india/article4901219.ece

true sense of technology "Information Technology Act, 2000" [Ita- 2000] was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes. The above Act was further amended in the form of *IT Amendment Act*, 2008 [ITAA-2008**]**.

The ITA-2000 defines 'Computer' means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network. The word 'computer' and 'computer system' have been so widely defined and interpreted to mean any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities and therefore any high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition.

The scope and applicability of ITA-2000 was increased by its amendment in 2008. The word 'communication devices' inserted having an inclusive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc like what was later being marketed as iPad or other similar devices on Wi-fi and cellular models. Though ITA- 2000 defined 'digital signature', however said definition was incapable to cater needs of hour and therefore the term 'Electronic signature' was introduced and defined in the ITAA -

2008 as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone.

The new amendment has replaced Section 43 with Section 66. The Word "hacking" used in Section 66 of earlier Act has been removed and named as "data theft" in this section and has further been widened in the form of Sections 66A to 66F. The section covers the offences such as the sending of offensive messages through communication service, misleading the recipient of the origin of such messages, dishonestly receiving stolen computers or other communication device, stealing electronic signature or identity such as using another persons' password or electronic signature, cheating by percolation through computer resource or a communication device, publicly publishing the information about any person's location without prior permission or consent, cyber terrorism.

The acts of access to a computer resource without authorization, such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus like Trojan etc. The offences covered under section 66 are cognizable and non-bailable. Whereas, the consequence of Section 43 of earlier Act were Civil in nature having its remedy in the form of damages and compensation only, but under Section 66 of the Amendment Act, if such act is done with criminal intention that is means area, then it will attract criminal liability having remedy in imprisonment or fine or both.

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC.

Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating.[159] agencies file the cases/ charge-sheet quoting the relevant sections from IPC under section 463,464, 468 and 469 read with the ITA/ITAA under Sections 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.

4.6 Position in the European Union Convention on Cybercrimes

This instrument is a product of Council of Europe whereby European Union Member States are signatory thereto. The Conviction behind establishing this instrument was to adhere to the dire need of pursuing of course as a matter of priority, a common criminal policy aiming at the protection of society against cybercrime, among many things, by having legislation and fostering International co-operation.[160]

---

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

[160] Preamble to the Convention on Cybercrime cited at http://www.coe.int/t/dghl/cooperation/economic crime/cybercrime/T-CY/Default-TC-en-cup

Article 2[161], the Convention provides that it is an illegal to access to computer system. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3[162] deals with illegal interception of communication system.

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent or in relation to a computer system that is connected to another computer system".*

Article 4[163] deals with data interference by deleting any information from the computer, damages or deteriorating the system without any right. This article 4 provides as hereunder,

> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when*

[161] Budapest Convention
[162] ibid
[163] Budapest Convention

committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 of the Convention deals with the System interference, Article 5 provides as follows and we quote it as hereunder:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 7 of the Convention deals with Computer related forgery and run as follows:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 of the Convention deals with computer-related fraud and provides as follows:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when

committed intentionally and without right, the causing of a loss of property to another person by:

a. *Any input, alteration, deletion or suppression of computer data;*
b. *Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.*

The Convention have identified other cybercrimes like child pornography, cyber terrorism, infringement of the copy rights example is the burning of CDs are some of cybercriminal conducts.

4.7 Conclusion

We have seen in this chapter that legislation in a number of countries as shown above exist to combat cybercrimes. It was shown that Malaysia, the European Union and the UK have a good piece of legislation for cyber crimes, which Tanzania may adopt.

CHAPTER FIVE

5.0 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusion

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

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

As observed in this Study, information technology has spread throughout the world. Now days, computers are used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development. As the user of cyberspace grows increasingly diverse and the range of online

interaction expands, there is expansion in the cyber crimes and as pointed out earlier, the financial sector is the main target. It is for this reason that there is need to adopt a strict law to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber crime. The United Kingdom has issued a law for cyber crimes since 1990. It was recently amended, in accordance with the European Convention on cyber crime, by *The Police and Justice Act* 2006. Chapter 48 which came into force on October 1, 2008. All aspects concerning cyber crimes were regulated.

5.2 Recommendations

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

1. The Penal Code should be amended to provide for criminal activities conducted using computers and computer networks.
2. The offences that should be introduced in the Penal Code are hacking, illegal access to computers and computer networks, fraud committed using computers and computer networks, money laundering and related crimes, identity theft, sniphing and many others.
3. It is not enough to amend the Penal Code, another law which is relevant to this study is the Criminal Procedure Act of 1985. It should as well be amended to provide for modern means of investigating cybercrimes.
4. International cooperation is also vital in cybercrimes. It is recommended that there should be a convention at the international level similar to the one which is operational in the European Union.
5. There should as well be training for judges, magistrates, investigators and prosecutors on cyber crimes.

REFERENCES

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

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

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

Cited at http:/allafrica.com/stories/201206270719.html.?aa-source=useful-column visited on 5th June, 2013 at 11.00am

Comer, M.J., (1985) *Corporate Fraud***,** Mc Graw Hill Book Company, 2nd Ed, London

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

Gibbons, J. H., (2004)"*Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity***",** U.S. Government Printing Office, Washington, D.C.

Gunarto, H., *Ethical Issues in Cyberspace and IT Society* Ritsumeikan Asia Pacific University

Heathcote, P.M., As Level ICT, Payne-Gallawary Publishers, Ipswish

http://allafrica.com/new/group/main/main/id/00021259.html? aa-source visited on 20th June 2013

http://dailynews.co.tz , visited on 6th June, 2013

http://dailynews.co.tz , visited on 7th June, 2013

http://dailynews.co.tz , visited on 7th June, 2013.

http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf visited on

7th July 2013

http://portalsandrais.frbatlanta.org/online-banking-fraud/ visited on 27th June 2013

http://rbidocs.rbi.org.in/rdocs/Bulletin/DOCs/6270.doc visited on 20th July 2013

http://rbidocs.rbi.org.in/rdocs/Bulletin/DOCs/6270.doc visited on 23th July 2013

http://www.afp.gov.au/national/major_fraud/internet_scams visited on 13th July 2013

http://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en visited on 30th July 2013

http://www.arraydev.com/commerce/jibc/) visited on 10th July 2013

http://www.bcs.org/server.php?show=conWebDoc.10452. visited on 15th July 2013

http://www.coe.int/t/dghl/cooperation/economic crime/cybercrime/T-CY/Default-TC-en-cup visited on 8th August 2013

http://www.coe.int/t/dghl/cooperation/economic visited on 10th August 2013

http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf visited on 20th June 2013 at 11:00am

http://www.legalindia.in/cyber-crimes-and-the-law visited on 5th August 2013

http://www.link.co.uk/Press/NewsReleases/Pages/Fraud_Prevention_Guide.aspx visited on 2nd July 2013

http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective visited on 8th August 2013

http://www.ukpayments.org.uk/payments_industry/payment_fraud/plastic_fraud/types_of_card_fraud visited on 5th July 2013

Kondobagil, J. (2007), *Risk Management in Electronic Banking; Concepts and Best Practices***,** John Wiley

Lloyd, I. J., (2000) Information *Technology Law*, Butterworth 3rd Ed, London,

Loudon, K. C. & Traver, C.G**. (**2008**),** *E-Commerce: Business, Technology and Society*, 4th Ed, Person Education International, New York

Mambi, A., *Shaping the Information Society, E-Children Protection, Legal Measures*, a Paper presented at IGF, 2nd Parliamentary Forum

Mwiburi, A.J., "Legal *Implications of Developments in Information and Communication Technology: An Appraisal of the Electronic and Postal Communications Act, 2010*

Prasana, A**.,** **"***Cybercrime: Law and Practice*" accessed at http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf

Singh, N. P., *Online Frauds in Banks with Phishing, Journal of Internet Banking and Commerce,* August 2007, vol.

Singh, Y.,(2012) "*Cyber Laws*,'' 5th Edn, New Delhi: Universal Law Publishing Co. Pvt. Ltd.,

Ubena, J. **"***Why Tanzania Needs Electronic Communication Legislation? Law keeping up with Technology" The Law Reform Journal*, Vol. 2, No.1, 2009, pg.

Viswaanathan, (2012), *A., Cyber Law, Indian and International Perspectives,* Lexis Nexis Butterworth Wandwa, Nagpur

www.allafrica.com. visited on 27th July 2013

www.arraydev.com/commerce/jibc/ . visited on 30th June 2013