CYBERCRIME AND CRIMINAL INVESTIGATION: CHALLENGES WITHIN THE TANZANIA POLICE FORCE FORENSIC LABORATORY: THE CASE TANZANIA POLICE FORCE HEAD QUARTERS, DAR ES SALAAM

CYBERCRIME AND CRIMINAL INVESTIGATION: CHALLENGES WITHIN THE TANZANIA POLICE FORCE FORENSIC LABORATORY: THE CASE TANZANIA POLICE FORCE HEAD QUARTERS, DAR ES SALAAM

By

John Mayunga

A Dissertation Submitted to Mzumbe University Dar es- Salaam Campus College in Partial Fulfilment of the Requirements for the Award of the Degree of Master of Public Administration (MPA) of Mzumbe University

2013

CERTIFICCATION

We, the undersigned, certify that we have read and hereby recommend for acceptance by the Mzumbe University, a dissertation entitled; **Cybercrime and Criminal Investigation: Challenges within the Tanzania Police Force Forensic Laboratory: The Case Tanzania Police Force Head Quarters, Dar Es Salaam** in Partial Fulfilment of the Requirements for the Award of the Degree of Master of Public Administration (MPA) of Mzumbe University.

……..
Major Supervisor

…….
Internal Examiner

……
External Examiner

Accepted for the Board of MUDCC

……
CHAIRPERSON, FACULTY/DIRECTORATE BOARD

DECLARATION
AND
COPYRIGHT

I, **John Mayunga,** declare that this thesis is my own original work and that it has not been presented and will not be presented to any other university for a similar or other degree award.

Signature_____

Date_____

ACKNOWLEDGEMENTS

First, I thank my supervisor Lucy Massoi, for her continuous support and intellectual insights; although she was away, still she listened, gave advice, wrote and commented. This dissertation would not have been completed without her professional advice and unfailing patience.

I must take this opportunity to express a special thanks to all my lecturers, friends and colleagues at Mzumbe University, Dar es Salaam Campus College who tirelessly offered encouragement and support when it was most needed.

A special thanks to my family for their help during the time of my studies; their encouragement and love was of great value. Special thanks to TCRA, NMB, Tanzania Posta Bank, CRDB and Cybercrime officers who responded and supported me throughout the data collections. Without their help the paper would have not been completed.

Finally, I am grateful to my wife for her humble support throughout my studies.

DEDICATION

I humbly dedicate this degree to almighty God who made it possible. Also I dedicate it to my beloved wife Annakleta Victor and our daughters Paskazia and Evelada for their strength and courage to endure the time of my studies.

ABBREVIATION AND ACRONMYS

£	-	Pound
ATM	-	Automated Teller Machine
BSA	-	Business Software Alliance
CRDB	-	Community Rural Developing Bank
DoS	-	Denial of Service
DPP	-	Director of Public Prosecution
EPOCA	-	Electronic Postal Communication Act
FATF	-	Financial Action Task Force
FBI	-	Federal Bureau Investigation
FBL	-	Forensic Bureau Laboratory
ICT	-	Information and Communication Technology
NMB	-	National Microfinance Bank
OECD	-	The Organisation for Economic and Cultural Development
TCRA	-	Tanzania Communication Regulatory Authority
TPB	-	Tanzania Post Bank
TPF	-	Tanzania Police Force
U$D	-	United State Dollar
UK	-	United Kingdom
UN	-	United Nations
USA	-	United State of America

ABSTRACT

The remarkable achievement in Information and Communication Technology sector in Tanzania and the world has changed the way of life socially, culturally, politically and economically. The technology contributed to emergency of modern crime known as "Cybercrime". Incidences of crime are disseminated in Tanzania and the world at a high speed.

The country, business agencies and individuals suffer from immoral activities their fellow Tanzanian and other foreigners have turned ICT in free area for commission of offence. In order to overcome the challenges of advancement of new technology on ICT, Tanzania needs to enact cyber law. The existing law in Tanzania has not sufficiently considered the online cyberspace and offence have changed from traditional to modern crime. The aim of this study was to investigate Cybercrime and Criminal investigation: The Challenges within the Tanzania Police Force Forensic Laboratory in Tanzania Mainland. Specifically, the study intended to identify three key issues: Firstly, factors accelerating the trend of cybercrime; secondly, the effects of cybercrime in Tanzania; and Thirdly, measures taken by the government to fight against the increase of cybercrime in Tanzania.

Both secondary and primary sources of data collected from cybercrime unit, Banks and TCRA in Ilala District Municipality were used in the course of this study. A total of 20 Cybercrime Officers, ten NMB Officers, ten CRDB Officer, ten TPB Officer and ten TCRA officers including junior and senior and Executive Officers were interviewed. Several research instruments were used, including questionnaires, interviews and the review of records. In a nutshell, findings revealed advanced technology, inefficient technological capacity, lack of cybercrime law and lack of knowledge as factors accelerating the trend of cybercrime in Tanzania Mainland.
Based on the study findings, the Government should enact cyber law to addresses the challenges of technological development based on cyber security in terms of knowledge and skills towards cybercrime.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

CHAPTER ONE

BACKGROUND INFORMATION

1.1 Introduction

This chapter introduces background information, statement of the problem, objectives of the study, research questions, and significance of the study, limitation, delimitation of the study, organisation of the study and important terms of the study.

1.2 Background Information

Globally, the evolution of ICT, markedly the internet, is transforming societies worldwide. It offers unique opportunities in terms of social, economic, cultural and scientific development (Pack, 2012/2013). KPM international, in 2011 there were 2 billion internet users and over 5 billion mobile phone connections worldwide. Everyday 294 billion e-mails and 5 billion phone messages are exchanged. Most people around the world depend on the consistent access and accuracy of these communications1.

The Secretary of State for the Home Department proposed that, internet has transformed the way millions of consumers buy goods and services. The UK is the leader in Europe in terms of the size of the internet shopping market, whereby, in 2008 the value of online sales was £48 billion. 57% of the UK order goods and services over the internet.

However, almost one in three UK internet users are not shopping online due to lack of trust, fear over personal security and lack of trust in companies selling over the internet. Cybercrime reduces the consumer confidence and the losses for credit card fraud of £308 millions in 2008. Stealing the innovation and design of music was estimated at £180 million in 2008. Rapid development of computer technologies and exponential expansion of the internet have spawned a variety of new technology

[1] Cybercrime-A Growing Challenge for Governments, KPMG International Corporation; July 2011, Vol. eighty.

specific criminal behaviours that must be included in the categories of computer crime (ASLAM, 2006). As business and society rely on computers and internet based networks, cybercrime and digital attack incidents have increased around the world. In 2008 the cost of cybercrime worldwide was estimated at approximately USD 8 billion. As for corporate cyber espionage, cyber criminals have stolen intellectual property from businesses worldwide worth up to USD 1 trillion (Interpol, 2012). These crimes includes financial scams, computer hacking, downloading pornographic material from the internet, virus attacks, e-mail stalking and creating websites that promote racial hatred. Cybercrime was reported in 2000, when a mass- mailed computer virus affected nearly 45 million computer users worldwide. In 2010, the global spam rate increased 1.4 percent year-on-year (KPM, 2010). Today cybercriminals are now moving beyond computers, and are attacking mobile handheld devices (KPM, 2010). In the US, over the course of one year, the cost of cybercrime newly doubled from US$265 million, in 2008 to US$560 million in 2009 (ICCC, 2010).

Most countries have not defined what computer crime is and how it differs from real world crime. ASLAM, (2006) Computer crime can be defined as a violation of criminal law that involves the knowledge of computer technology for its penetration, investigation, or prosecution. The cybercrime Convention of the Council of Europe 2001 does not directly define cybercrime, but it makes provisions for those activities that member states are required to legislate. These include Illegal access, Illegal interception, Illegal interference, System interference, Misuse of device, Computer related forgery, Offence related to child pornography, Offence related to infringements of copyright and related rights, and Attempt and aiding and abetting. Therefore, Convention defines cybercrime as the prohibited act on the use of computer system for the crimes (Oluwabukola)2

[2] Oluwabukola Adelaja..Catching up with the rest of the world: The Legal framework of cybercrime in Africa

In African context, as observed by Oluwabukola Adelaja Africa is a fertile ground for cybercrime because of the developed technology, high crime rate and legislation. Cybercrime is growing at a faster rate in Africa than in any other continent in the world. Cyber security experts estimated that 80 percent of the computers in Africa are already infected with viruses and other malicious software.

Therefore, the African continent is vulnerable to cybercrime threats, due to the increased number of "new" internet users who are not security savvy. Cybercrime is not known to the vast majority, due to little understanding knowledge, lack of security awareness, shortage of local cyber security experts and a lack of funds (Pack, 2012/2013).

In Tanzania, the cybercrime unit was inaugurated in 2006 in the Police Force Forensic Laboratory, aimed at fighting against computers related crime. In Tanzania, internet users, population and Facebook statistics for Tanzania internet were 4,932,535, in 2011 and Facebook users were 437,040 in 2012 (Pack, 2012/2013). Similarly, the cybercrime unit reported that over 18 million people are connected to mobile phone networks, and 8 million are connected to the internet.

An increased trend of cybercrime in Tanzania threatens National security. Lack of knowledge or limited awareness of new technologies led to bank and mobile consumers to be victims of cyber criminals. However, the impacts of cybercrime continue to grow. The threat frustrates the network security and business system including home computers. The trend for growth in cybercrime and digital devices is increasing in 2012, 387 cases were reported by the Tanzania cybercrime unit. Inter alia offences are stealing; obtaining money by false pretence, Computer/ATM fraud, Computer theft, Publishing of Obscene Communication, computer forgery and Threaten to kill via Electronics Device (SMS), and these are the most leading computer and digital device crimes in Tanzania.

Country wise, trends of cybercrime cases are increasing year to year as per Tanzania cybercrime Unit statistics. In 2007, 270 cases were reported; in 2008, 382 cases; in 2009 351 cases; in 2010, 444 cases and in 2012, 542 cases were reported. According to the cybercrime unit report (2012), Regional Trend of Computer Related Crime Cases, Dar es Salaam has experienced an increased rate in on cybercrime. In 2007, 31 cases were reported; in 2008, 45 cases; in 2009, 40 cases; in 2010, 50 cases and in 2012 54 cases were reported. In Mwanza in 2007, 12 cases were reported; in 2008, 39 cases; in 2009, 35 cases; in 2010, 40 cases and in 2012 45 cases were reported. In Dodoma in 2007, 32 cases were reported; in 2008, 21 cases; in 2009, 22. Cases; in 2010, 31 cases and in 2012 38 cases were reported. In Mbeya in 2007, 28 cases were reported; in 2008, 32 cases; in 2009, 30 cases; in 2010, 30 cases and in 2012, 35 cases were reported. In Arusha in 2007, 7 cases were reported; in 2008, 22 cases; in 2009, 23 cases; in 2010, 30 cases and in 2012, 35 cases reported. In Mara, Singida, Manyara, Mtwara and Ruvuma very few cases are reported over cybercrime. This trend shows that cybercrime rate is fuelling up in the big cities.

The Tanzanian Deputy Minister of Home Affair reported that 500 people were apprehended for cybercrime after the strengthening of the cybercrime unit between 2011 and 2012. Due to rapid technology advancement Tanzania has had many cases inside and outside of cybercrime (Majaliwa, 2012). The law of most countries do not prohibit cybercrime and mechanisms of cooperation across national borders are complex (Goodman, 1997).

"Cybercrime", "computer crime", "Information technology crime" and "High-tech crime" are synonymous and refer the two kinds of crime. First, the computer is the target of the offence with attacks on network confidentiality, integrity and illicit tampering with systems, programs or data (Goodman, 1997). Second are economic offences (fraud, theft, industrial espionage and sabotage), infringements on piracy, propagation of illegal and harmful contents, facilitation of prostitution and other moral offences and organized crime. Therefore an adequate framework of cybercrime law is an absolute prerequisite for effective action against cybercrime.

1.3 The statement of the problem

In a digital era of computers, the government faces an increased of risk of cyber-attack (Kshetri 2010). This is constantly growing with new opportunities to commit old crimes in new ways. Tanzania lost Tsh 892.18 billion on cybercrime and Tsh 250 million were reported stolen through ATMs (Mwananchi, Monday 16 July 2012)3. The major contributing factor of cybercrime in Tanzania is the absence of cybercrime law and cybercrime policy which is viewed as a gap. Lack of knowledge and limited awareness of the new technology contributed to bank and mobile consumer victims of Tsh 2.2 billion (Mwita, 2012). Criminals found that the internet is less controlled and see it as a place where they can commit crime anonymously. Hackers steal a total of 1.3 billion online and US $551,777 and 8,897 Euro through cybercrime (citizen correspondent, Monday, January, 7th 2013). The crime persists because most users have little knowledge of sophisticated ICT-related services. Paganinip (2012) argued that "cybercrime growth has been fuelled by an evident lack of adequate protection. Cybercrime is a global phenomenon, which needs joint effort. According to the Chief of the Forensic Bureau, online patrol training to police officers will improve the effectiveness and efficiency in fighting crime (Majaliwa, 2011). The government of Tanzania in collaboration with other stakeholders has started to implement reform aimed at addressing incidents of cybercrime. Despite the concerted efforts by authorities at national and international levels, resource constraints and gaps in existing law hamper the prosecution of much of today's cybercrime (BSA, 2007).

Therefore, the interest of this study was to examine the challenges of cybercrime to criminal investigation in Tanzania. It is an emerging research area in Tanzania and with increasing reported cases of such crimes, and advancement in ICT from the late 1990s, it provides a room for research to find out the reason for this social problem.

[3]Mtambalike (2012). Tanzania Lost 892.18 billion on Cybercrime Last financial year; "Mwananchi" Local news paper on Modern, 16 July 2012 accessed online at http:www.tech 360 magazine.wm/2012/07/Tanzania- lost 89218-billion-on-html.

1.4 Research objectives

1.5 General objective

The broad objective of the study was to investigate the challenges of cybercrime to criminal investigation officers in Tanzania Mainland.

1.6 Specific objectives

In order to accomplish the above general objective, the study had the following specific objectives:

(i) To identify factors accelerating the trend of cybercrime

(ii) To identify the effects of cybercrime in Tanzania

(iii) To identify measures taken by the government to fight against the increase of cybercrime in Tanzania

1.7 Research questions

(i) What are the factors accelerating the trend of cybercrime?

(ii) What are the effects of cybercrime in Tanzania Mainland?

(iii) What are the measures taken by the government to fight against the increase of cybercrime in Tanzania?

1.8 Significances of the study

The study intended to collect data in order to analyse the real factors influencing the trend of cybercrime in Tanzania. The study is significant in the following aspects:

One, to gain knowledge of skills needed for the improvement of the Cybercrime Unit in the Department of Criminal Investigation. Two, at the governmental level, the results will assist Government agencies to be able to investigate and prosecute all cases concerning cybercrime that happen online. Three, policy makers will discover the need for national cyber security policy that will provide the framework for the application of computer and digital devices in communication. Four, the study will at the end investigate the importance of training in the performance of forensic services in the criminal investigation system in Tanzania. In this regard, results will also suggest the best way to improve the forensic performance and effectiveness of its services.

1.9 Limitation of the study

The researcher encountered the following limitations. There was a lack of enough funds to accommodate transport, stationeries and meal for the researcher.

1.10 De -Limitation of the study

Although cybercrime has no boundaries, the researcher, was however, limited to the Dar es Salaam Region of Tanzania Mainland. The accessibility of information in those places, the targeted officers and people were easily accessible in the regions. The selected boundaries reduced the cost of transportation and saved time. The sample size of the studied population also helped the researcher meet the Mzumbe University calendar on time.

1.11 Organization of the dissertation

This dissertation is organized in six chapters. Chapter one covers the background of the problem, statement of the problem, objectives of the study, research questions, limitation, delimitation of the study and organization of the study. Chapter two presents the conceptualization of cybercrime; theoretical studies the current literature from different studies for various sources, empirical review and literature gap on the challenges of cybercrime to criminal investigation officers, the subject matter of this study. Chapter three covers the manner in which the study was conducted. The key components included research design used in this study, population, sampling procedures, sample size, data collection methods and data analysis. The research methodology was based on both qualitative and quantitative analysis. Presentation and analysis, and analysis of findings obtained from the respondents by the researcher in the in statistical indexes, tables, graphs, used in order to support the literature and respondents assumption of the problem. Chapter four presents the findings and discussion on the trend of cybercrime, factors accelerating the trend of cybercrime in Tanzania Mainland, the effect of the cybercrime, and the measures used towards cybercrime. Chapter five presents the discussion and findings of the study. Chapter six covers the summary, conclusion and policy implications.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter presents the conceptualization of cybercrime; theoretical studies the current literature from different studies from various sources, on the challenges of cybercrime to criminal investigation officers which is the subject matter of this study.

2.2 Conceptualization: Cybercrime

Danquah and Longe, (2011) argued that cybercrime is a global phenomenon where technology and the Internet is used and its impact cannot be over emphasized. Therefore we need to harmonize law and develop International Corporation in order to effectively investigate the problem. Cybercrime is defined as any criminal act dealing with computer or computer network (e - crime, computer crime, or internet crime in different jurisdictions). Schell and Clemens (2004) defined cybercrime as a crime related to technology, computers and the internet and it concerns governments, industries and citizens worldwide where cybercrime takes the form of either piracy, preaching (obtaining free telephone calls), cyber stalking, cyber terrorism and cyber pornography. However, any activity uses the internet to commit crime (Milhon, 2007). Pant, at el., (2012) argued that, cybercrime includes but is not limited to; theft of telecommunication services; communication in furtherance of criminal conspiracies; information piracy; counterfeiting and forgery; dissemination of offensive materials; electronic money Laundering and tax evasion; sales and investment fraud; illegal interception of telecommunications; and electronic funds transfer frauds. Clough (2010) Cybercrime encompasses three typologies of Cybercrime as summarised by the US Department of Justice; crime in which the computer or computer network is the target of the criminal activity. For example, hacking, malware, and DoS attack, existing offences where the computer is a tool used to commit the crime. For example child pornography, stalking criminal, copyright infringement and fraud, crime in which the use of computer is an incidental

aspect of the commission of the crime but may afford evidence of crime (Clough, 2010).

2.3 Theoretical studies

This paper reviewed the theories of crime that have been applied to the study of cybercrime. Many theories have been developed in an attempt to explain why crimes occur. This study applied self-control theory and routine activity theories to explain why cybercrime occurred. They focus much on individual level characteristics in individuals or the situations that increase the chances of a crime occurring. The study of cybercrime will become more important as we look for solutions to this growing problem. According to classical theorists people will not participate in crime if they know what the punishment will be. Before examining the different theories that have been applied to the study of cybercrime it is helpful to understand the different schools of criminological thought. In criminology the two main schools of thought are the classical school and the positivist school. Classical theorists believe that people are rational and that they commit crimes through their own free will in order to satisfy their own self- interest (Cullen & Agnew, 2012:27). According to Classical theorist people will not participate in crime if they know what punishment will be. Therefore people rationally choose to participate in acts. In order to prevent the act from the occurring people need to know that the consequences will outweigh the benefits. If people believe that the consequences will outweigh the benefits they will freely choose not to participate in criminal behavior (Gzsybrowsk, 2012:27).

2.3.1 Self- Control Theories

One general crime theory that has been applied to the study of cybercrime is the self-control theory was proposed by Travis Hirschi and Michael Gottfredson in 1990 and published in A General Theory of Crime (Gzsybrowsk 20012:27). This theory believed that criminal is rampant, but the people acts on this motivation only when they posses low self-control (ibid). This paper discussed the basic elements of the self-control theory, as well as research that provided evidence to support the validity of this theory. This paper will review the empirical studies that have been applied in

self-control theory to the study of cybercrime and cyber victimization will discuss the study of cybercrime (Gzsybrowsk, 2012).

Individuals with low self-control are impulsive, insensitive, physical (as opposed to mental), risk taking, short sighted and nonverbal, and they will tend therefore to engage in criminal and analogous acts (Gzsybrowsk 2012:28) therefore they are likely to participate in deviant behavior because they want immediate gratification. Individuals with self-control characteristics are able to delay immediate gratification and are more likely to be vigilant, emotional, verbal, and long-term oriented. Individuals with self-control may be better able to appreciate the consequences of participating in deviant acts and have the control necessary to delay their gratification.

In their theories Hirsh and Gottfredson attested that individuals are not born with a certain level of self-control, rather they learn self-control through their parenting and develop differently. As they grow older they may develop different levels of self-control than when they were younger. Individual differences may have an impact on the prospects for effective socialization (Gzsybrowsk 2012:29). People make a choice whether to commit crime or not to, the decision is made based on the cost and benefit analysis (Danquah, et al, 2012). Scientists use this approach to understand human behaviour, in the rational choice theory. The scholar comment in relation to cybercrime for example the electronic mechanism such as the use of automated access control system and surveillance camera can serve as deterrents because they increased the perceived risk of being apprehended. Theory explains more on the process of criminal and the decision to commit crime which is a problem to cyber. In order to teach the community self-control, someone must monitor behavior, recognize deviant, and punish behaviour, all this requires active systems and deficiencies to any of these systems may lead to development of low self-control (Gzsybrowsk 2012).

Lack of self-control makes crime more attractive to an individual who possesses learned characteristics such as impulsivity and lack of responsibility, good parenting and care leads to development of an individual with high self-control and who is able to monitor, recognize and effectively punish deviant behaviour. This is consistent with the result of Wada and Odulaja (2012) who attested that, the response of technology to cybercrime problems centre on the use of computer security theories to design and evolve solution that provides authentication verification, non-repudiations and the models rely on the use of cryptography, steganography, network protocols, and the use of software engineering process models to develop systems that offer some forum of protection for users and the information infrastructure.

Cybercrime thrives on the web today because the internet did not inculcate in the protocols from the onset a mechanism that allows a host to selectively refuse a message. No society can afford to accuse criminal matters without duly accepting its responsibilities. Social control theory stresses on the fact that most delinquent behaviour is the result of unmonitored "social control" by the authorities and primarily the family. The relationship and commitment with respect to set of norms and beliefs structure encourage or discourage individuals and group to break the law (Danquah et al, 2012). Pratt and Cullen (2000), in their study, they found that lack of self control is a strong predictor of involvement in crime. Self control is useful in explaining why individuals participate in criminal behaviour while others do not.

The researcher also found that self-control is not the only predictor of deviant behavior, but that variable from social learning they are also useful in explaining individual participation in deviant activities Pratt and Cullen (2000). Criminal behavior cannot be explained entirely by one theory; it requires the interconnection of various theories. Self-control theory is an important factor in predicting criminal activities. Therefore, some researcher extended to the self-control theory the study of why some individuals commit cybercrime such as Higgins and Makin 2004, Higgins, 2005; Wolfe and Marcum 2008; Moon, Morris and Higgins 2009; McCluskey and McCkluskey 2010, (Gzsybrowsk, 2012). One empirical study of 358 college students found that individuals who possessed characteristics of low self-control were likely to

commit crime of digital piracy (Gzsybrowsk, 2012). Another study applied self-control theory of cybercrime to find that individuals with low levels of self-control were likely to view online pornography than individuals with high self-control (Buzzell, 2006). Therefore the application of self-control theory can help the researcher understand better why individuals participate in deviant online behavior and suggest possible ways of combating cybercrime. That is why the researcher decided to apply this theory in the study of cybercrime and criminal investigation: The challenges within the Tanzania Police force Forensic Laboratory.

2.3.2 Routine activity theory

The study reviewed crime theories that have been applied to the study of cybercrime. Over the past two hundred years many theories have been developed in an attempt to explain why crimes occur. Some of these theories, like self-control theory and routine activity theory, have been applied to the study of cybercrime. These theories focus on the individual level characteristics in individuals or the situations they are in that increase the chances of a crime occurring. The theory proposed three situations facilitating the occurrence of crime. Proponent argued that such events must happen at the same time and in the same space. These situations are the existence of suitable target, lack of security and a motivated offender for the crime to occur. The assessment of the situation determines whether or not a crime takes place (Wada & Odulaja, 2012). Similarly, Danquah et al (2012) argued that a crime must occur where there is an opportunity for a crime to be committed. Although it is not true that crime occurred in an opportunity as argued in routine activity theory but crime occurred due to human behaviour.

Outlaw (2001) Routine activity theory has been criticized by several authors as one, focus on demographic variables as proxies for activities or lifestyle, presuming that a certain way of life characterizes different demographic groups rather than identifying specific measures of guardianship or target suitability, Second, many studies do not identify and measure activities that are directly relevant to the type of crime under study. That is, when the routine activity measures merely differentiate certain ‘types’ of people (e.g., young men) from others or simply assess risk by ascertaining the

amount of time people spend at home or 'out', it is left unclear whether the results can be understood as supporting routine activity theory. The strength of the applications of the routine activity theory is that it identifies specific types of activities or lifestyle factors that may put individuals at risk for a certain type of crime either because they lower the potential for guardianship or because they increase target suitability (Outlaw, 2001). Routine activity theory describes the situational factor that must be present for a crime to occur in conjunction with self-control theory; routine activity theory can help explain why cybercrime occurs. Therefore, the applications of these theories are of great importance to the researcher and the policy maker in thinking of good control methods that are appropriate to the combating of cybercrime in Tanzania mainland.

2.4 Factors accelerating the trend of cybercrime in Tanzania

Tanzania is lacking cyber law, in order to protect the national infrastructure and the safety of citizens against the threat offered by cybercrime and technology related criminality, national cybercrime strategies must be developed, and the need of practical knowledge on cybercrime and experienced personnel must be addressed. It is important to develop the National policies and strategies on the prevention and control of cybercrime (Paganinip, 2012). Paganinip (2012) Argued that the great influence of both the nature and scope of current and future crime is technology, and the influence of technology on future of crime can be demarcated into three categories;

(i) Advancements in technology will continue to provide criminals the tools to facilitate the commission of traditional crime such as fraud, theft, money Laundry, and Counterfeiting;

(ii) Technology itself will be the target of criminal offence such as theft of telecommunications' services and the spread of viruses;

(iii) New technology will be used to prevent or deter criminal attack.

Access to more precise information about the true incident of cybercrime would enable law enforcement agencies to better prosecute offenders, deter potential attacks and enact more appropriate and effective legislation. It is uncertain to what extent

cybercrime is reported, not only in surveys but also to law enforcement agencies. Authorities engaged in the fight against cybercrime encourage victims of cybercrime to report the crime. Though, the developing ICTS did not consider about cybercrime, for criminal method and new method of investigating cybercrime. However the increasing number of internet users causes difficulties for law enforcement agencies because it is relatively difficult to automation investigate process. Other factors contributing to cybercrime include globalization, whereby the advancements in telecommunications, international trade, travel, and immigration have resulted in irrelevance of national borders, at least as far as crime is concerned. Moreover the internet has been a boom particularly for international crime, allowing offences from different countries to group together more easily by overcoming geographical limitation. Additionally, more offences can be committed without the perpetrator ever having entered the jurisdiction where the crime has occurred. Increased international migration, mobility of individuals, families and large grouping of people will continue to fuel crimes related to illegal immigration, in particular migrant smuggling (Paganinip, 2012).

An Increase in the occurrence of cybercrime is due to the lack of deterrence factor on the internet which creates the opportunity for users to perpetrate in cybercrime. This is consistent with the social control theory that, online delinquent behaviour is the result of unmonitored social control by constituted social network and the community as a whole. Tripathy and Mishra, (2013) argued that "one of the major rise of identity fraud was due to increased internet transition, that reduces human contact and reduces the opportunity for identification of checks". Moreover online banking, electronic financial transaction, online data stores and internet commerce have become popular and the technologies to prevent misuse continue to expand, hence led to financial loss. Olowo (2009) Cybercrime is motivated by fraud, typified by the bogus emails sent by "phisher" that aim to steal personal information. The explosive growth online fraud made "phishing" and to a lesser extent "pharming" part of nearly every internet user's vocabulary in most recent time. Furthermore Phishing and pharming are forms of fraud aimed to dupe the victim into believing that they are viewing a trusted

website such as their banks, while in fact it is a bogus website that intended to steal custom identity and drain their financial information.

Paganinip (2012) observed that one principal for the increase in counterfeiting in recent years is the advance in such technologies as personal computer, scanners, colour laser printing, photocopiers and desktop publishing software. The decreased cost of these tools have increased their accessibility and also opportunities to commit a number of frauds-related crimes, which was once the domain of highly skilled forgers or counterfeiters who required specialised equipment and expertise. Cyberspace is a place where cyber activity takes place; it's a convenient but fictitious notion describing the network of networks' constituting internet, the communication and service provided through it. Therefore it is difficult for the state and their law enforcement agencies to trace apprehend and punish perpetrators of cybercrime beyond their respective territories, because the very nature of international law, a state sovereignty is limited to its territory (Olowo, 2009).

Olowo (2009) commented that the source and target of cybercriminal activity is the growth of international banking activity and Money-Laundering as the unique opportunity of a quickly developed financial infrastructure allowing anyone to transfer monetary fund to any state, through tangled route have caught the attention of cybercriminals. Electronic transfers are an efficient tool in concealing the source of money intakes and in Laundering illegally earned money. Similarly, Longe and Chiemeke (2008) proposed that Internet currently serves as a hiding place for fraudster who has simply migrated from the street to an electronic platform offered by the World Wide Web. However, crime is direct opposite to development, because it leaves a negative social and economic consequence.

Lack of adequate security in wireless networks leads to criminal attacks such as theft of data, corruption of system integrity, hacking, sabotage, espionage, theft of capacity, and loss or theft of mobile and portable devices. This will facilitate the increase in unauthorized access to information held on the network, unauthorized creation or modification of data on the network, and Denial of Service (DoS) attack

on the network or other networks unauthorized access to a network can be send spam or other messages, download or distribute illegal contents such as child pornography launch further attacks or engage in other online criminal acts. (Gregor &Krone, 2006) Longe and Chiemeke, (2008) this explains the unpreparedness of society and the world in general towards combating crimes. However the crime prevailing in Tanzania today are computer related crimes as the Tanzania Police Cybercrime unit statistics trends shows that there is an increase in crime year-to-year. Cybercrime seems to yield much to criminals in developing nations such as Tanzania, therefore it is not going to be curbed easily because the offline criminals have gone high - tech and are making "huge money" from the business (Longe & Chiemeke, 2008).

Professor (2010) establishes that, implementing cyber security measures requires skilled manpower, however most countries including Tanzania face a shortage of skilled people to counter such cyber-attacks". Ronald Noble, Head of Interpol, argued that "there is shortage of skilled and experienced personnel to fight this type of crime not only at Interpol but in Law enforcement everywhere". In Australia, majority of incidents particularly minor incidents are not investigated due to lack of forensic skills and expertise. Also cybercrime investigator experienced a problem in its performance that is, a lack of personnel, limited budgets, and limited resources for training as well as slow and time consuming Paganinip (2012). Moreover, the performance of cybercrime investigation depends on the quality of its staff and the determination and motivation of its Leadership; cooperation with prosecution, courts and other agencies at the domestic level; cooperation with the private sector and international cooperation (ibid).

Computer crimes are difficult to prosecute due to nature of technology and unfamiliarity of the law enforcement with technology. Law enforcement agencies are burdened with cumbersome mechanisms that are accustomed to dealing with real-world crimes. The trans-border nature of computer crime further enhances the difficulties, because the traditional assumptions; being observed preparing for , committing and/or being seeing fleeing from an offence no longer hold (ASLAM, 2006). Similarly, it is also argued that, the development of Information and

Communication Technology particularly the internet, where transactions are online based and don't require physically seeing the person, criminals found the internet to be less controlled and see it as the only place to commit crime anonymously (Athumani, 2012). Moreover, an underground economic provides the tools and infrastructures to commit cybercrime over computer systems, sending spam , spreading malware or carrying out denial of services attacks, market for credit cards that can be used for identity-related fraud, or money mules to move crime proceeds and lends criminals money. The Underground market used to be accessible for a select public with proper connections, but nowadays they are more accessible for everyone with bad intentions (Paganinip, 2012). In my opinion Shortage of trained, skilled, and knowledgeable law enforcers who can tackle problems based in current technology, identity theft, white collar crimes, and cybercrime can also linked with the fuel that increases the trends of cybercrime. New technologies often require a high level of education and training to use them effectively. But this is a problem to police agencies as well as until automated systems become available to help monitoring incoming data much of the information collected by camera and other tools will be used more to provide evidence for prosecutions than to prevent or interrupt crimes (Osborne et al, 2008).

Klerk and Kop (2008) advanced forms of telecommunication can facilitate crime, certainly when use is made of powerful encryptions, because criminals can operate faster and shield themselves better and use the technology to supply disinformation to shield their own activities or obstruct the investigation and legal action. According to International Telecommunication Union, (2009) law enforcement agencies need adequate instruments to investigate potential criminal act such (data detection) that can interfere with the rights of the innocent.

Ipu et al (2011) established that lack of sufficient resources for instance, funds which would enable authorities to purchase equipment's and applications necessary to collect evidence and also applications and instruments to detect and prevent such crime from happening are quite limited. Also authority or other lack necessary skills that afford them the capacity to employ efficient strategies in detecting and collecting digital evidence crucial in prosecuting cyberspace offence.

Therefore capability on applying this method to acquire evidence needed, this method required to investigate computer forensic include;

(i) Analyzing hardware and software used by the suspect in the commission of crime
(ii) Supporting investigation in identifying relevant evidence
(iii) Recovering deleted files
(iv) Decrypting files; and
(v) Identifying internet users by analyzing traffic data.

Also, Broadhurst and Roderic (2006) observed that preserving a chain of evidence is a great challenge to investigation. Almost every case will soon require computer forensics, and evidence will be located in multiple places. The challenges facing investigators is information management against cybercrime. Such as offence against the confidentiality, integrity and availability of computer data such as illegal access of computer system; interception of non-public transmission of computer data to form, or with a computer system; interference with computer system; interference with operator system such as a sabotage, and misuse of computer related devices including the production, sale, and procurement for use, import or distribution of such devices. Similarly, Ally (2011) argued that integrity and confidentiality of data is an issue in many court cases. Hackers gained access to a computer system that contains records of people. Therefore Tanzania needs cyber law that will criminalize the saboteurs, hackers, crackers or computer trespassers in Tanzania. As observed by Gregor & Krone (2006) law enforcement agencies have limited power and capacity to monitor electronic signals for signs illegal activities. These law enforcers depend to a large extent on complaints from the public, and computer users are often unaware of intrusion on their wireless networks or unwilling to report them. Furthermore, the rate of reporting attacks on computers to police is low particularly by organizations that experienced electronic attacks or other form of computer crime within their work place do not report the attack to law enforcement.

Krone and Urbas (2006) establish of wireless systems installed by home users, businesses and other institutions have obvious advantages in terms of convenience and access, but the feature increased the risks of outside intrusion and misuse. Therefore law enforcement needs to be aware of the way in which criminals have begun to exploit the vulnerabilities of these new forms of information and communication technologies. Additionally, all major forms of cybercrime today have one thing in common "They are an industry for organized gangs who specialized in one particular activity and share tools with one another to accomplish their crime". Therefore, we need a holistic approach to address cybercrime threats and the steps that they can take to stay secure, providing technology that is resilient to attacks and enabling law enforcement to investigative and prosecute cybercriminals (Business Software Alliance 2007).

Kwak et al (2005) establish the main problem that faces the law enforcement for that kind of crime will, no doubt is place for transnational computer crime as well;

(i) Law enforcement is not sufficiently trained or adept at responding to technological or organizationally complex crime

(ii) Law enforcement is faced with significant "regulation conflict" arising from international and inter-organizational relationship underlying transitional computer crime. And with these difficulties, a compounding problem for law enforcement aiming at transnational crime is that research is very limited.

Furthermore, it is hard to convict a cybercriminal because of two major reasons: firstly, few countries have enacted e-law and the existing ones are not sufficient in convicting culprits because of jurisdiction anomalies especially when the investigation transcends international borders. Secondly, obtaining evidence of computer crime that would stand in courts of law is lacking in many countries like Tanzania since the field of computer forensic is still relatively new and lacks sufficient literature and expertise. Cybercrime poses a serious threat to the security of cybercitizen and all countries should take it seriously (Ipu et al, (2011).

Information awareness is crucial for combating cybercrime. In Tanzania, there is significant lack security awareness, and leaving the business across countries vulnerable to cybercrime online attack. This is due to inefficiency in the Information and communication technology security awareness program that is available in English. Therefore we need strongly ICT security awareness training to educate users, employees and law enforcers to understand the risks and prevent attack. Cybercriminal are looking for the sites that have many users with poor security awareness to infect, and social networking sites are an excellent place to hunt (Longe & Chiemeke, 2008). Mehta and Singh, (2013) comment that lack of awareness about the internet, and low levels of internet security provide an important heaven for cybercriminals. However the growing number of computer crimes is due to lack of knowledge on rapid development of cyber-attacks globally. On the other hand the increased use of modern technologies without proper cyber security, expert and cyber law stirred computer criminality to propel.

Similarly lack of awareness of the incoming cyber threats and contraction of investment in prevention and control has fuelled cybercrime. Since transactions takes place online without physically seeing the person. Similarly, Mathew (2012) argued that cybercrime persist because most users have little knowledge about sophisticated ICT- related services in varies sphere of economy. Inability to use ATM cards, for example some clients ask for assistance from other people, this escalates fraud and loss of ATM cards. Pack (2012/2013) established that lack of Functional Computer Security Incident Response Team in Tanzania was identified as a major issue and unimplemented National awareness program addressing major risks facing the users. Specialization within Tanzania Police Forces is limited; the criminal investigations department is responsible for investigation of all cases regardless of seriousness and nature of the crime, TPF lacks investigative and prosecution capacity which is regarded as the serious impediment to the delivery of effective and efficient criminal justice. Some crimes are not prosecuted due to lack credible evidence, due to poor investigation techniques coupled with a limited forensic capacity (Robison 2009). Law enforcement agencies in many jurisdictions have been unable to respond

effectively to cybercrime and even in the most advanced nations including the developing countries particularly Tanzania (Broadhurst & Roderic, 2006).

2.5 The effect of cybercrime

Salifu (2008) observed that about 200 countries are connected to the internet; therefore cybercrime has become a global issue and requires full participation of the stakeholders. Information and infrastructure security is a nation's ability to deter, detect, investigate, and prosecute cybercriminal activities. Business Software Alliance 2007 in their reports argued that cybercrime today is "overwhelmingly fuelled by profit, employs sophisticated technologies capable of highly personalized attacks, and increasingly emanates from organized crime". Moreover, the raised vast, surreptitiously controlled computer networks have led to exploitation in the number and type of cybercrime committed.

Without doubt, the financial damage caused by computer and internet crime is significant various publication analysed the impact of cybercrime, the Computer Crime and Security Institute analyse the economic impact of cybercrime based on the 494 respondents of computer Security practitioners in its corporations, government agencies and financial institutions. In 2006 total losses amount to some USD 66.9 million based on financial fraud, viruses and theft of confidential data and system penetration by outsiders. The FBI Computer Crime Security 2005 estimated the total loss for the United State economy, and the assumptions that more than 20% of US organizations are affected by computer crime; a total of loss of USD 67 billion was stolen Ipu et al (2011) they argued that, cybercrime poses a greater threat to the national security of all countries, even technologically developed like USA. Additionally abuse and misuse of computer system have existed nearly since mainframe computers were first invented during the 1940s and 1950s a means to improve military munitions and then rocket guidance system. In 1970s researchers began studying computer crime because in those days harmful activities committed with computers were not prohibited by computer crime laws. By the 1980s change began bypassing computer law that's based on computer hackers and soon expanded to other behaviour (Ipu et al 2011).

Curtis et al (2000) observed that many estimated cost for economic crime trends be over $500 billion annually. The significant increase in trends, in 1970s cost was approximately $5billion; it rose to $20billion in 1980s and $1000 billion in 1990s. This increased economic crime has a serious effect on the economy. The estimated fraud loss for the credit card industry amount to $1.5billion annual, of which $230 million for online transactions and MasterCard reported to be 33.7% increased worldwide fraud from 1998 to 1999. Ipu et al (2011) they observed moral panic fuelled by media about effect of pornography in the mid-1990s, the threat to child safety from pedophiles. The emergence of the world wide web, along with myriad of software applications, online content, began of broadband internet connector, computer crime has evolved into computer related crime and then whats called cybercrime. Therefore, Cybercrime has become a global issue and new affecting almost all the countries. In Australia for example, a study conducted revealed that 67 percent of respondents said that they had been victim of computer and cybercrime (Urbas, 2001) as cited in (Salifu, 2008).

Salifu (2008) argued that a Metropolitan Police officer told the group of investigator about the fast growing problem of identity theft, banks were quiet about attacks on their systems because of public confidence, and lacked confidence in the ability of police to deal with such crime. For example the cost of identity theft to the UK economy would be much greater than the official figure of £ 1.7 billion a year. The US president Bill Clinton allocated US$ 1.4 billion in 1990 to improve government computer securing against the risk of cybercrime (Salifu, 2008). And in India a computer engineer was charged with allegedly stealing 100 hours of internet time from a client (Hindu, 2000, cited (Salifu, 2008).

Salifu (2008) the threat of cybercrime and other information security breaches continues unabated and the financial toll is mounting. Computer Crime and Survey conducted by US Federal Bureau of Investigation, the threat of cybercrime and other information security breaches continue unabated because cybercrime can be committed at any time anywhere and authorities charged with investigating it need to

spend more time and effort, compared to traditional crimes, to located and detect offenders. Police and security officer for example need to learn how to locate electronic evidence and deal with cross-border issue in tracing suspected hackers or crackers. Cybercrime is associated with high rate of unemployment, harsh economic conditions, and poor education system. Unemployment was linked with boredom, poor self-esteem and poor self-confidence. There is a slogan that say "an idle mind is the devils workshop" because most of the time youth use their time and knowledge to plan criminal activity in order to shape their livelihood and make ends meet (Schnierer and Vivian, 2010).

2.6 Measures taken by the government to fight against an increased cybercrime

2.6.1 International measures in combating cybercrime

In 1985, General Assembly resolution 40/71 of 11 December called upon Government and International organisation to take action in conformity with the recommendation of the commission on the legal value of computer record, in order to ensure legal security in the use of information processing in international transaction. In 1990, the General Assembly of the UN adopted the guideline concerning computerised personal data file. UN proposed to respond positively to protect the file against both natural and artificial crimes. Also UN manual on the Prevention and Control of Computer – Related Crime, presented a proper statement of the problem at the international level, activities based on harmonizing substantive law and establishing a jurisdiction base. The European Union also undergo the series of action to tackle cybercrime through impelling a coordinated law enforcement and legal harmonization policy that deals with confidentiality and security of processing personal data against cybercrime (Ally, 2011).

Broadhurst and Roderic (2006) The Interpol's General Secretariat has also supported the formation of regionally organised working groups comprising local experts in computer related crime who meet periodically to share experiences and develop best practice. Interpol is facilitating the exchange of information coordinating joint

operation activities of member states, and developing and sharing expertise and best practice covering wide range of criminal offence. A high effective approach to intergovernmental law enforcement condition that offers temperate for transnational cooperation against cybercrime is the Financial Action Task Force (FATF) established at G7 Paris Summit in 1998 and based in the OECD (The Organisation for Economic and Cultural Development). However the FATF is a policymaking body with the aim of implementation of legislation and regulator reforms needed to combat money Laundering. In 1960 OECD was established, and established a presence in law enforcement has been active in the area of cybercrime and online security especially in regard to encryption technology evaluating the balance between law enforcement and privacy concerns and the means by which member state can coordinate encryption policy.

G8 senior experts group on transnational organised crime, at the Halifax summit in 1995, G8 heads of state established a cross disciplinary group of senior experts to address methods of combating transnational organised crime. In 1996, the Lyon Group devised 40 recommendations aimed at increasing the efficiency of collective action against transnational organised crime via two International goals; strengthening capacity in investigation and prosecution of high-tech crime, and more effective regime for cross border cooperation in criminal matters. Broadhurst and Roderic (2006) as cited Grabosky Broadhurst 2005) outline the basic elements of effective regime for regional cooperation in combating cybercrime that include the following;

(i) improve security awareness by providing adequate resources to secure transactions and equip system operators and administrators;

(ii) improve coordination and collaborations by enabling systematic exchanges between the private sector and law enforcement including joint operation;

(iii) take steps to ensure that technology does not outpace the ability of law enforcement to investigate and enact substantive and procedural law adequate to cope with current and anticipated manifestation of cybercrime;

(iv) Broadly criminalize the conduct and focus on all violators big and small;

(v) Strengthen international initiatives by updating existing treaties and agreements to recognise the existence threats and transnational nature of high-tech computer crime and strive for legal harmonization and;

(vi) The development of forensic computing skills by law enforcement and investigative personnel and mechanisms for operational cooperation between law enforcement agencies from different countries.

Paganinip (2012) Developing of correct level of cybercrime legislation is the foundation upon which all other national and cooperation activities described by different researchers. Without legislation being in place other activities will not be implemented. However the specialists of cybercrime unit should contribute to the drafting of national legislation in the area of cybercrime. In many countries and particularly Tanzania, due to a lack of understanding of the issues, by legislators, certain cybercrime offences are not considered predicate offence for organised crime. Therefore the Government of Tanzania new about the increasing trends of cybercrime in the country and need to have cyber law in place. This need to be done in collaboration with other stakeholders against these technology inspired cybercrimes in Tanzania (Methew, 2012). Forensic study was a new field in developing countries including Tanzania, due to changing forms, trends and models of crimes, furthermore, the launching of forensic bureau particularly cybercrime unit in 2006 enabled to unmask the magnitude of cybercrime threats (Mirondo, 2010). Online patrol training was one of the plans by the Police Force in improving effectiveness and efficiency in executing their duty of fighting crime in the country (Majaliwa, 2011).

Building a knowledge based society is among the sub pillars of the Tanzania Vision 2025, which "envisages Tanzania developing into an information and knowledge based society with a vision to have a universally accessible broadband infrastructure and ICT as well as expertise to enhance sustainable socio-economic development and accelerated priority reduction nationally and become ICT development hub regionally" (Hassan, 2009). It is unconscionable that cybercrime is going unpunished (Business Software Alliance, 2007). The technology alone is not the answer as a

government must adopt stronger cybercrime legislation in order to have a rule to protect and serve in the digital world. Therefore international cooperation and uniformity in laws and punishment is needed in order to counter today's most sophisticated cybercrime threats (ibid). However, Dave De Watt establishes that there is a tremendous need for targeted legislation, modernizing current law and stiffening criminal penalties is key to enhancing our ability to pursue cybercriminals and stem the tide of cybercrime.

Dror and Charlton, (2006), expert performance and accuracy is an important issue in almost all specialization domains. In similarly to novice, experts should possess abilities and skills that enable them to perform certain tasks, such as cybercrime. An expert needs not only knowledge, but skills, judgment, and experience to evaluate, and interpret information correct decision. However, being an expert does not necessarily mean error-free performance. In most case the personnel recruited in Tanzania Police Force Forensic Laboratories are form four level that had not any addition skilled on the application of scientific machines, such as computer and other devices, handling and packaging of exhibits concerned cybercrime cases. However, Anderson argued that, you cannot be a forensic scientist without first being a scientist and a very good and well educated scientist as you will not only be analyzing and interpreting evidence which could be responsible for setting a person free or imprisoning them for life, but also you will and should be challenged to the utmost during cross-examination in court.

Cybercrime unit have inadequate incentives to produce reliable analyses of police evidence because they do not qualify to be forensic expert. Competitive self-regulation improves forensics by creating incentives for error detection and reducing incentives to produce biased analyses. Furthermore, the researcher argued that, forensic analysis often depends too much on the personal qualities of each individual forensic scientist. Idiosyncrasy of individual forensic scientists may determine the final result, and there is limited criticism, Forensic science is sometimes unreliable because the larger environment of knowledge seeking is not appropriately structured.

2.6.2 Africa countries and cybercrime initiatives

Some of African had moved ahead in taking initiative to combat cybercrime. South Africa, due to its advancement in economy, experience rapid increased in cybercrime. The country manages to pass the electronic communication and Transaction Act in 2002, that enable and facilitate electronic transactions to enforceability, and it create public confidence in electronic transaction. Also South Africa form alliance with European countries and is the only African country to ratify European Cybercrime treaty which outlaw cybercrime and provide member treaty to make laws criminalizing cybercrime and cooperate in combating cybercrime. In country like Nigeria cybercrime legislation, there are over 100 Information Technology related bills before legislation. None of which have been passed some are the cybercrime and critical infrastructure bills, computer security protection bills and electronic transaction bills. Lack of legislation will hinder the expansion of broadband network (Adelaja, Oluwabukola, n.d). Kenya passed communication and information Act into law in 2008 to govern and regulate the Telecommunication Sector in country, no specific provision that prohibit cybercrime in the law. In Tunisia, was the top most to African countries to deployment of ICT in its economy in development of enabling environment and infrastructure it enacted electronic commerce law 2000. Cameroon, deal with cybercrime activities through its Ministry of Post and Telecommunication and the National Agency for Information and Communication Technologies advanced to bill to the parliament that allow to set up cyber police force to define major crime, determine legal procedures to help fight cybercrime. The Government of Tanzania enacted Electronic Postal Communication Act (EPOCA) 2010 and Ant-Money Laundering Act 2006 in order to mitigate the problem of cybercrime in Tanzania. However, the TCRA in collaboration with Police is trying to find ways on how to manage protecting the consumers of communications services with the borderless crime (Guardian correspondent, February, 8 2013).

Liganga (2012) the judiciary in Tanzania has tried in certain instance to resolve the challenges such as ICT; by interpreting and applying the existing statutory and common principles in ways and manner that incorporate the existing social realities. Current law do not protect consumers against risk involved in the distance selling and

buying business because online or distance contracts were not in practice in Tanzania by the time these laws were enacted. Tanzania law neither cover online contracts nor recognise cyber- space. Tanzania law provide that contract must be in writing and dully signed or authenticated before witness. The report from the Tanzania Police Force shows that there is an increased in reported cases of computer related crime in the country. A good example of the increase of number of trader forging receipt imported goods using computer in order to evade tax. The incident of theft that occurred at Barclay bank where an organised group of business stole US$ 1.8 million, the same as Tanzania shillings 2.4 billion using technology is a continuation of computer crime taking place in Tanzania.

The US and UK, the government and institution rely on ICT have tried to employ computer experts who realise the risk of having attack before occur or before the security breaches and have enacted cyber law. But that have never be done in Tanzania and it remain clear, although the regulation of ICT in Tanzania is at initial stage, and much need to be done in the ICT legal frame work. The problem of cybercrime in Tanzania is the same as in many other jurisdictions increasingly fatal. But the law have never changed to reflect this dangerous advancement unfortunately until now, no specific provision in the penal code which addresses cybercrime as an offence under the code.

Makinde et al., (2012) comment that there is possibility of individuals, public and private sector within and outside the country, causing a loss of financial and physical damage. Furthermore due to cybercrime, a loss of billions dollars had been observed globally. Therefore cybercrime threaten the nation's security and financial health of public and private sectors due to the fact that hacker steal confidential information and future plan of the organisation and sale to another agency and in turn reduce the confidence of the agency.

2.7 Empirical Studies

Tanzania was expected by the end of 2009 to have completed the project of the optic fibre cable, the researcher argued that other developing countries like Tanzania are

likely to experience a rapid cybercrime grow as a broadband technology takes off. Crime proliferation is associated and facilitated by growth of broadband network (Nir 2010). Until now Tanzania does not have specific legislation deals with cybercrime, most of the laws were enacted before cyber security, the statutory laws have remained in yesterday after money at speed of light (Liganga, 2012). Flexibility provides some measures of discretion in law to make it adaptable to social conditions, but if law is rigid and unalterable it may not respond to changes (ibid).

Cybercrime unit was inaugurated in 2006 within the Tanzania Police Force Forensic Bureau Laboratory. According to Tanzania Police Force annual crime report of 2007, cybercrime unit managed to investigate 270 cases of computer related crime and handheld devices. In 2008, Annual crime report of Tanzania Police Force observed that 382 cybercrime was reported and investigated at the Forensic Bureau Laboratory. The Tanzania Police Force annual crime report of 2009 reported 351 cases of cybercrime all over the country, although it was reported that these are some of that cases that had been reported to Police station, though many cases are unreported.

Furthermore, Tanzania Police Force annual crime report (2010) noticed an increase of the trend of cybercrime up to 444 cases reported to Police stations, 542 cases reported in 2011 and 387 cases reported in 2012. Therefore cybercrime trends show to increase consecutively within the four as reported in different Police annual crime report of every year. As observed by Robison (2009) that investigation and prevention crime by TPF is compromised by poor investigation techniques, lack of both forensic capacity and expertise in handling evidence. In most case the personnel recruited for in the Tanzania Police Forensic Laboratory are form four level that had no any addition knowledge on the application of scientific machines, handling and packaging of exhibits. However, Anderson argued that, you cannot be a forensic scientist without first being a scientist and a very good and well educated scientist as you will not only be analysing and interpreting evidence which could be responsible for setting a person free or imprisoning them for life, but also you will and should be challenged to the utmost during cross-examination in court.

The FBLS, for criminal investigation department, "forensic workers have inadequate incentives to produce reliable analyses of police evidence" because they do not qualify be forensic expert. Competitive self-regulation improves forensics by creating incentives for error detection and reducing incentives to produce biased analyses (Koppl, 2005). Furthermore, the researcher argued that, forensic analysis often depends too much on the personal qualities of each individual forensic scientist. Idiosyncrasy of individual forensic scientists may determine the final result, and there is limited criticism, Forensic science is sometimes unreliable because the larger environment of knowledge seeking is not appropriately structured.

2.8 The Literature gap

There are very several publications about cybercrime and criminal investigation: the challenges within the TPF forensic laboratory such research are; Policy Brief, Addressing the challenges of law enforcement in Africa including Tanzania, the impact of ICT revolution in Tanzania's legal system; a critical analysis of cybercrime and computer forensic evidence and the impact of internet crime on development. However, very few publications that described the challenges of cybercrime to criminal investigation officer for example Robinson (2009) published a report titled as Policy Brief: Addressing the challenges of law enforcement in Africa including Tanzania and Ally (2011) with the report titled as the impact of ICT revolution in Tanzania's legal system; a critical analysis of cybercrime and computer forensic evidence and the impact of internet crime on development just few to mention. Cybercrime can be controlled, if we enact cyber law and formulation of national cyber security policy that will be implemented. Also the Government should focus on hiring skilled and knowledgeable personnel who will be dealing with cybercrime in public and private sector to fight against cybercrime. Therefore with reference to the identified gap, researchers need to conduct survey and come up with empirical data that will help to combat or reduce the cybercrime in Tanzania.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlined the manner in which the study was conducted. The key component included was the research design used in this study, population, sampling procedures, sample size also it includes data collection methods and data analysis. The research methodology was based on both qualitative and quantitative analysis. Presentation and analysis and analysis of findings obtained from the respondent by the researcher in the in statistical indexes, tables, graphs was used in order to support the literature and respondents assumption from the problem.

3.2 Research Design

Research design as the detailed blue print used to guide a research study towards its objective (Aaker et al, 2002, Adam & Kamuzora, 2008). It constitutes the blueprint for the collections, measurements and analysis of data (Kothari, 2004 as cited in Adam & Kamuzora, 2008). Other researcher refers as to a survey because it concerned with collecting information from a targeted size of cases, unit or inquiry under investigation (Kothari, 2004). The study intended to investigate the challenges of cybercrime to criminal investigation officer in Tanzania Mainland. The researcher was used both qualitative and quantitative research design. The importance of research design is to provide a research paradigm and relevant evidence that should be collected in relation to minimum expenditure of time, money and effort.

3.2.1 Case study Research Design

Adam and Kamuzora (2008) argued that there are four specific research designs to be considered in developing research strategy which are method design, sample design, analysis design, and organisation design. Other designs were case study research design, Survey Research design and experimental research design. A case study research design is an intensive description and analysis of a single situation. Case studies frequently use qualitative data, but also quantitative research can be used.

Therefore case studies involve in-depth, contextual analysis of similar situation in other organization, where the nature and definition of the problem happen to be the same as experienced in the current situation. (Adam & Kamuzora, 2008).

Therefore this research adopted case study research design because it is fairly exhaustive and enabled the research to study deep different aspects of cybercrimes; the design is flexible in respect to data collection methods and it save both time and cost of the study due to its nature of concentrated on a single issue.

3.3 The study area

The research was conducted in Dar es Salaam City, particularly in Ilala district at the Department of Criminal Investigation, Tanzania Police Headquarters particularly in cybercrime unit.

3.4 The Study Population

The population of this study comprised officials from police cybercrime unit, and officials from NMB, CRDB, TPB, and TCRA. The sampling technique was non-probability sampling (purposive) was used in which the researcher selects elements of which she /he believe they will be able to deliver the required data. The researcher used this technique because he wants to get the required data on the factors influencing cybercrime among the e-banking user in Tanzania.

3.5 Sample size and Sampling technique

3.5.1 Sample size

The sample of this population involved 20 officials from cybercrime units, 10 officials from NMB, 10 officials from CRDB, 10 officials from TPB, and 10 officials from TCRA. This sample is very representative in a sense that there are males and female respondents.

3.5.2 Sampling Procedures

This is a process by which a researcher uses to get sample from large population of studies. Komb and Tromp (2006) argued that, it is a process of selecting a number of

individual or objects from a population such that the selected group contains elements representative of the characteristics found in the entire group for the purpose of this study a researcher will decide to use both purposive sampling and simple random sampling techniques. The reason for selecting these methods is simple in application and somehow they reduce sampling error, in purposive sampling the researcher chooses only element which he believes would deliver the required data (Adam and Kamuzora, 2008). Similarly, Kombo and Tromp, (2006) states that, the "advantages of simple random sampling are that the sample yield research data that can be generalized to large population" so these methods was suitable for this study.

3.6 Source of data

3.6.1 Primary Data

Primary data is the data collected by the researcher himself/herself or by the research assistants from the field for the purpose of answering a research question (Adam & Kamuzora, 2008). Therefore the data collected from the field answered the issues of Cybercrime and Criminal Investigations: The challenges within the Tanzania Police Force Forensic Laboratory.

3.6.2 Secondary Data

Secondary data were data obtained from literature sources or data collected by other people for some other purposes (Adam and Kamuzora, (2008). The researcher reviewed and surveyed files and various documents, which was relevant information on my study. The documents involve the administrative documents, polices, training manual, file, books newspaper, articles, and report of Cybercrime unit, and Police Annual crime reports. However the information obtained intended to answer the issue of Cybercrime and Criminal Investigations: The challenges within the Tanzania Police Force Forensic Laboratory.

3.7 Data collecting Methods

The research applied multiple methods in collecting accurate and reliable information, this includes; interview, documentary analysis, and observation was

used (Adam and Kamuzora, 2008). The researcher of the study is going to use interview, and questionnaires. Kothari (2003) explain that, interview involves the presentation of oral verbal stimuli and reply in terms of oral-verbal. It uses personal interview to allow the researcher to be flexible when asking questions. She/he can start at the beginning, end or middle (semi- structured interview).

The nature of question asked clear and short to facilitate the analysis of data. This helped respondents to give corporation hence they are not forced in answering all questions. Questionnaires designed to respected respondents as pointed out in the random sampling. There were type of the questionnaires distributed to officials of cybercrime units, NMB, CRDB, TPB, and TCRA.

3.8 Data collection Instruments

The Instruments which used on this study was as follows: interviews, questionnaires and documentary guide.

3.8.1 Interviews

Kothari (2003) explain that, interview involves the presentation of oral verbal stimuli and reply in terms of oral-verbal. An interview is a major instrument through which information obtained from Ilala District in Dar es Salaam city. The interview was both formal and informal; due to the limit of time of the study, interview have the advantage of having greater flexibility, allowing control of the interview situation, guaranteeing a high response rate, and allowing the researcher to gather supplementary information (Kothari, 2000). It is the most effective methods of collecting large quantities of in-depth data and the researcher would not spend long time in field (Barners, 2001).

3.8.2 Questionnaires

Kothari (2000), contends that, this instrument consists of a number of questions printed or typed in a definite order on a form or set of forms. This instrument was used to collect information in all objectives. The respondents questionnaires was printed in English, since from the pilot survey conducted by other researchers showed

that respondents have knowledge of English Language. Questionnaires were designed to respected respondents as pointed out in the simple random sampling. Questionnaire is a widely used instrument in a survey design, close ended questions were used in this study which obtain specific numerical, nominal and ordinal data that respondent required to answer in terms of 'yes' or 'no'. Also open ended questions were used in this research where a respondent was requested to answer questions about specific issues about academic performance. The respondents provide answers to the questions in forms of opinions, views, suggestions or recommendations and were recorded in form of statements or numerical values. There was set of questions designed to collect information from the officials of cybercrime units, NMB, CRDB, TPB, and TCRA regarding the cybercrime and criminal investigation: the challenges within the Tanzania Police Force Forensic Laboratory (see Appendices).

3.8.3 Documentary review

The secondary data of the study based on quantitative method of secondary sources, this part comprised of reviewing different literature on cybercrime and criminal investigation; the challenges within the Tanzania Police Force Forensic Laboratory.

3.9 Data Analysis

The study was mainly quantitative and qualitative but some descriptive statistical was emanate in quantitative to indicate some data. The data from questionnaire and interviews was classified first according to the specific objectives. Tables, percentage were used and coding for qualitative data. Those data which was collected by the researcher in the field was generally quantitative data and were processed through SPSS software for analysis. Therefore ddata analysis refers to examining what have been collected in survey or experiment and making deductions and inference. The data collected was logging, coding, adjusting, and formatting (Adam & Kamuzora, 2008). In this study data analyzed, and presented in Table, bar charts, percentage and frequencies. However data summarized, and analyzed quantitatively by utilizing the data processing software such as SPSS and Microsoft excel to determine the descriptive statistical analysis.

3.10 Ethical consideration

These are codes of conducts in any research. The study never uses techniques to create false impression or deception, For example, data manipulation or fabrication without going to the area of study. Respondents were given the freedom to speak and answer the researcher depending on the nature of the question. The researcher concentrated on the data related to the challenges of cybercrime to criminal investigation officer in Tanzania Police Force Laboratory. The researcher never interfere respondent's privacy. The data collected in this study would only be used for the purpose of this study. Respondents to be interviewed never disclosed their anonymity. The studies never use plagiarized material when collecting data.

CHAPTER FOUR

PRESENTATION OF THE FINDINGS

4.1 Introduction

This chapter presents the findings obtained from the case area. The chapter is organized as follows: characteristics of respondents, the trend of cybercrime, factors accelerating the trend of cybercrime in Tanzania Mainland, the effect of the cybercrime, and the measures towards cybercrime.

4.2 Characteristics of Respondents

4.2.1 Sex

In Table 4.2.3 shows that 68.3 percent of the respondents survey were male, while Female were 21.7 percents. The analysis revealed that the number of female studying computer science is low compared to male, which create unequal opportunity between the sexes. However majority of the respondents work in Cybercrime unit as shown in Table 4.2.

4.2.2 Age Distribution

Of 60 respondent surveyed 55 percents were of the aged between 29 and 38 years, 18.3 percent aged 39-48 years, 8.3 percent were between 49-58 years, and 1.7 percent aged 59-68 years and over 68 years old were 3.3 percent as shown in Table 4.2.3 below. The analysis showed that 55 percent of the respondents surveyed were of the age between 29 and 38 years old.

4.2.3 Education Level

In all the respondent survey 40 percent were Postgraduate, and 23.3 percent were Graduates as shown in Table 4.2.3 below. Majority of the surveyed respondent are postgraduate.

Table 4.2.3: Characteristics of Respondents (N=60)

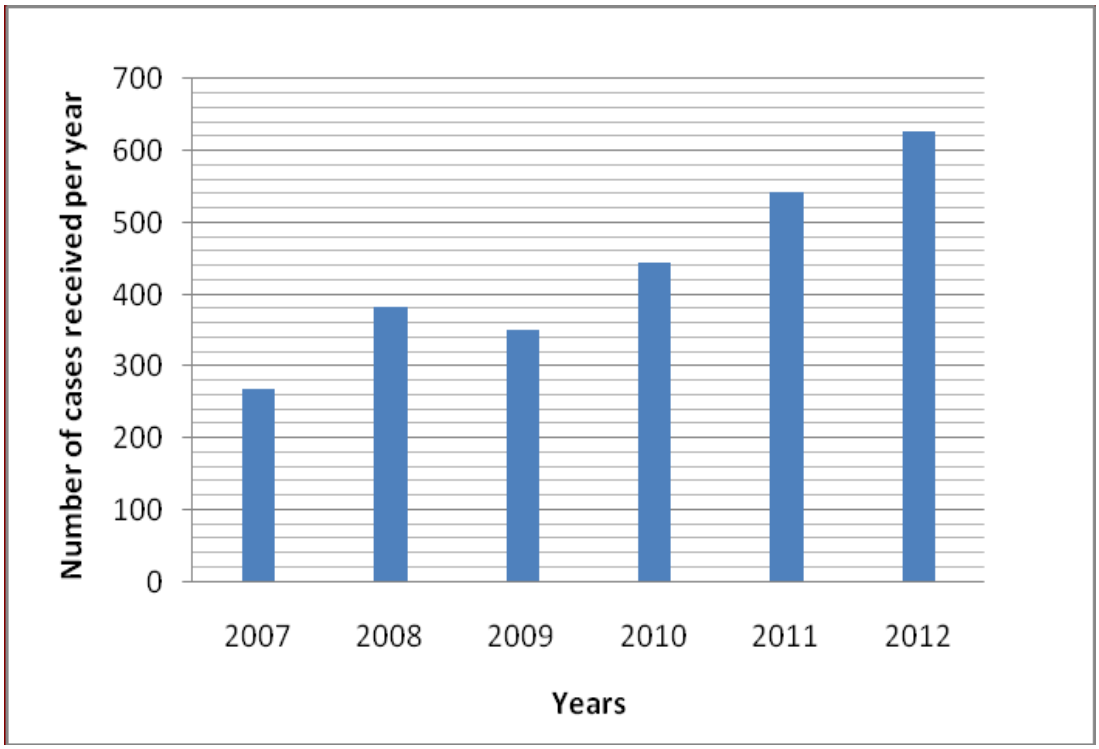
		Frequency/%	Percent
Sex	male	41	68.3
	female	13	21.7
	Missing	6	10.0
Age	18-28 years	8	12.7
	29-38 years	33	55.0
	39-48 years	11	18.3
	49-58 years	5	8.3
	59-68 years	1	1.7
	over 68 years	2	3.3
Education	Primary education	1	1.7
	Secondary education	6	10.0
	College education	14	23.3
	Graduate	24	40.0
	Postgraduate	14	23.3
	missing	1	1.7
Unit	Cybercrime	20	33.3
	Risk management	29	48.3
	Fraud	4	6.7
	ICT	5	8.3
	Operation card	1	1.7
	Broadcasting	1	1.7

Source: Researcher (2013)

4.3 The trends of cybercrime in Tanzania Mainland

The analysis from documentation showed that Tanzania mainland experienced increased trends of cybercrime at an average of 436 which is equal to 16.6 percent for six years consecutively. Whereby, in 2012, 627 cybercrime cases were reported to police station as shown in Figure 4.3 below.

Figure 4.3: Shows the Trend of Cybercrime in Tanzania Mainland (N=60)

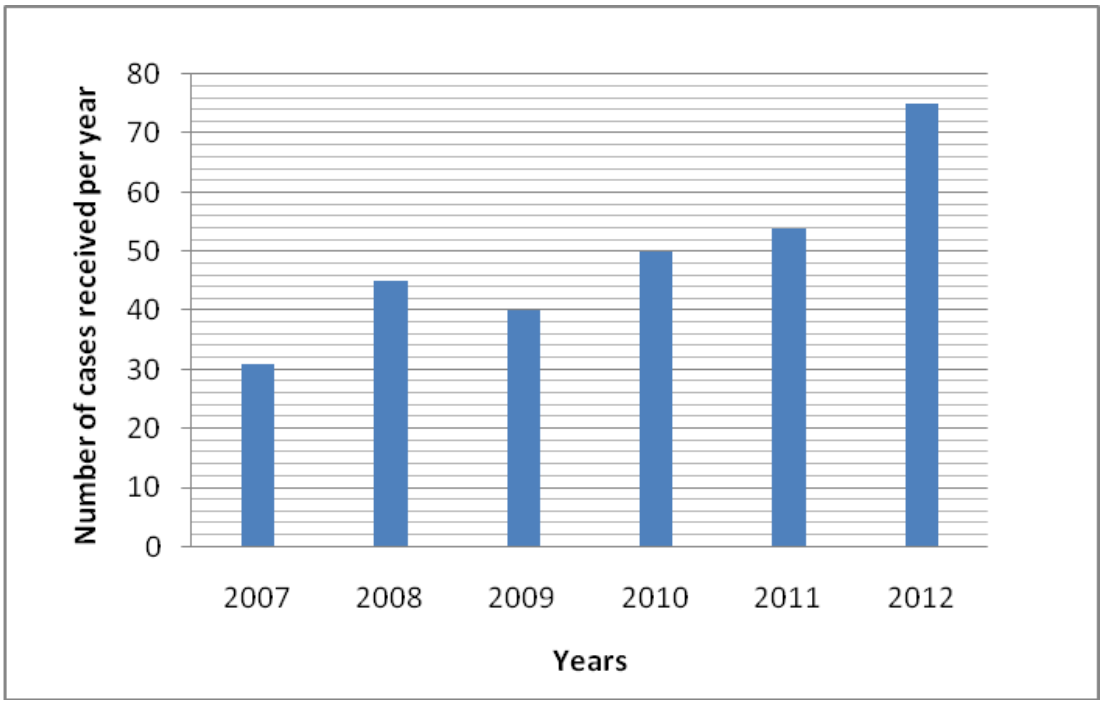


Source: Tanzania Police Force Annual Crime Report (2012)

4.3.1 The trend of cybercrime in Dar es Salaam

The analysis of secondary data showed that Dar es Salaam experienced an increased trend of cybercrime cases at an average of 49 cases which is equivalent to 17 percent of the total case of cybercrime in six year consecutively as shown in Figure 4.3.1 below.

Figure 4.3.1: The Trend of Cybercrime in Dar es Salaam (N=60)



Source: Tanzania Police Force Annual Crime Report (2012)

4.4 Factors that accelerating the trend of cybercrime

One of the objectives of this study was to identify factors accelerating the trend of cybercrime. The respondents from Police, TCRA, NMB, CRDB and TPB were asked to respond on the factors that accelerating the trend of cybercrime in Tanzania mainland as shown In Table 4.4 below, 85 percent of the respondents said they are unaware of the factors that accelerating cybercrime while 15 percent said they know and this factors includes; new technology, electron banking system and internet banking, financial gain, insufficient technology capabilities, electronic storage of valuable information, unemployment and the foreigner with knowledge of how to temper with ICT see Table 4.4 below.

Table 4.4: Factors that accelerates the trends of cybercrime (N=60)

Factors	Respondents	Percent
new technology	17	28.3
electron banking system and internet banking	14	23.3
financial gain	6	10.0
lack of cybercrime law	7	11.7
unemployment	2	3.3
foreigner with knowledge of how to temper with ICT	2	3.3
Insufficient technological capabilities	9	15.0
electronic storage of valuable information	3	5.0
Total	**60**	**100.0**

Source: Researcher (2013)

Also, the researcher wanted to know if the trend of cybercrime was decreasing in Tanzania mainland. As shown in Figure 4.4 below, 85 percent of the respondents said that the trend of cybercrime was not decreasing while 15 percent argued that it was decreasing. Majority of respondents mentioned the following as the reasons to the trend of cybercrime, as lack of knowledge of ICT, increased usage of technology in daily activities, lack of cyber laws, increased number of victim and case reported to Police, technological advancement and electronic financial accessibility.

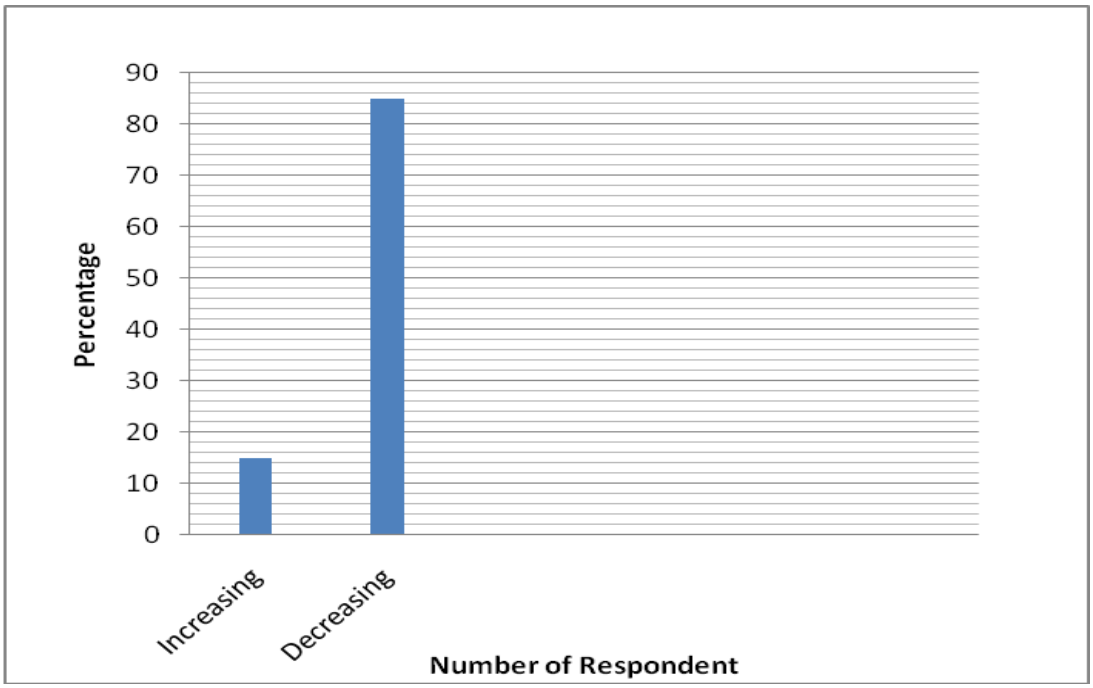
Table 4.4 show other factors that contributed to the trends of cybercrime are lack of ICT knowledge, increased usage of technology in daily life, lack of cybercrime law, increased number of victim and case reported to police, technological advancement and electronic financial accessibility.

Table 4.4: Factors Contributing to Cybercrime

Responses	Frequency	Valid Percent
Lack of knowledge on ICT	8	13.3
Increased usage of technology in daily activities	9	15.0
Lack of cybercrime law	4	6.7
Increased number of victim and case reported to police	15	25.0
Technology advancement	21	35.0
Unemployment	2	3.3
Electronic financial accessibility	1	1.7
Total	**60**	**100.0**

Source: Researchers (2013)

Figure 4.4: Show Awareness of the Trend of Cybercrime (N=60)



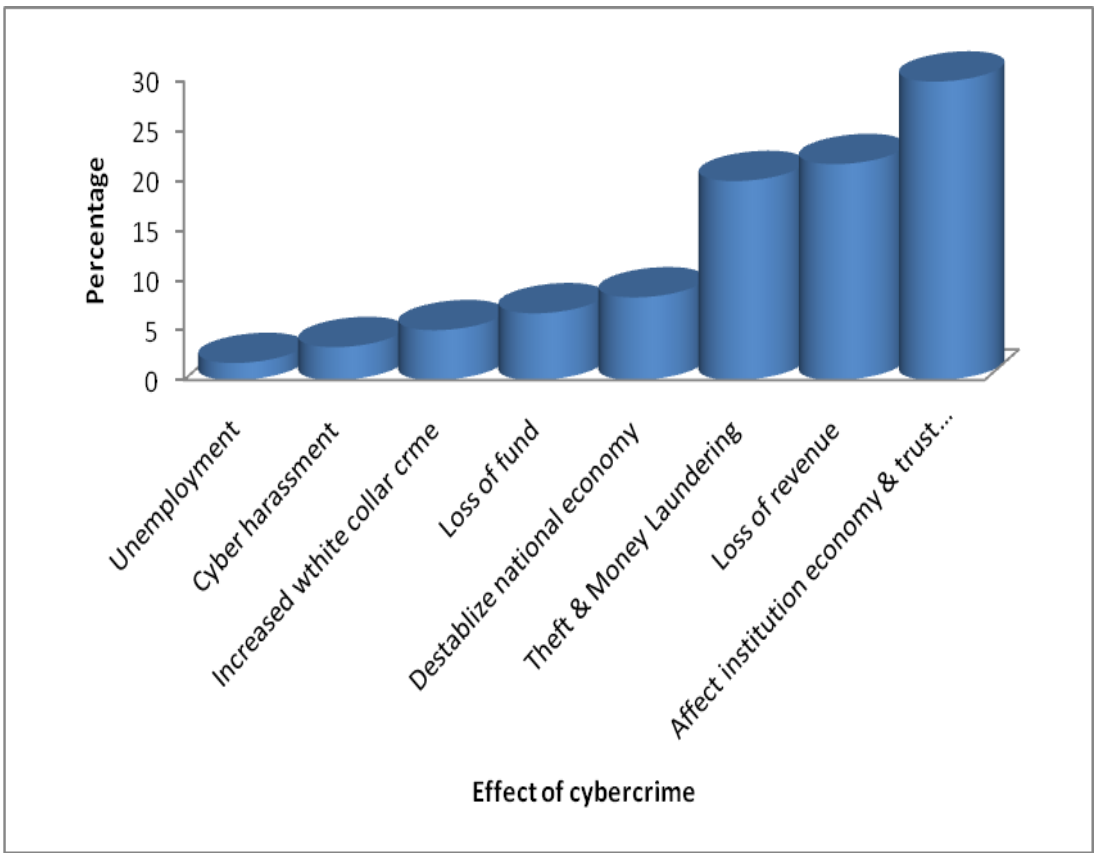
Source: Researchers (2013)

4.5 The effect of cybercrime in Dar es Salaam

This is another objective of the study that aimed to identify the effects of cybercrime. The analysis in Figure 4.5 below shows that 83.3 percent of the respondents are not aware while 15 percent said that they are aware of the effect of cybercrime. However,

Table 4.5 and figure 4.5 below; shows the effects of cybercrime as, theft and money laundering, loss of fund, increased white collar crime, cyber harassment, loss of revenue, destabilization of the national economy, affect the banking sector economy and trust to customer and unemployment. However 30 percent of the respondent said that cybercrime affect the banking economy and trust to the customer.

Figure 4.5: Show the Effect of Cybercrime (N=60)



Source: Researchers (2013)

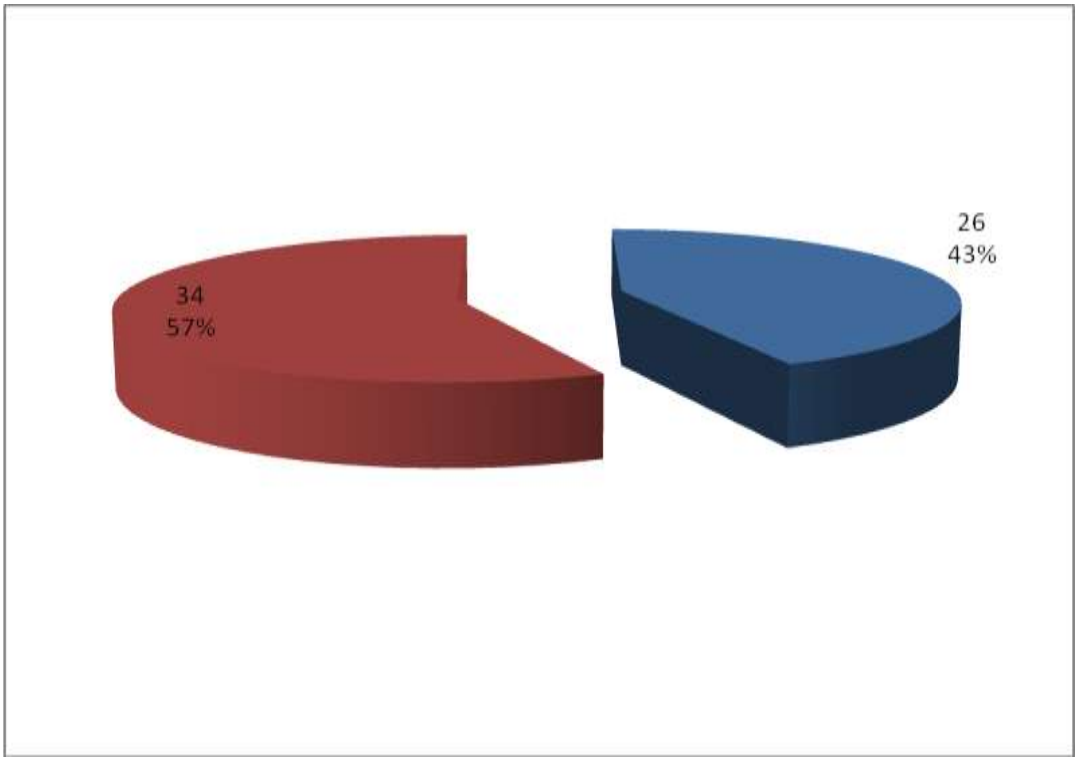
Table 4.5: Show the Effects of Cybercrime (N=60)

Responses	Frequency	Valid Percent
Theft and money laundering	12	20.0
Loss of fund	4	6.7
Increased white collar crime	3	5.0
Cyber harassment	2	3.3
Loss of revenue	13	21.7
Destabilization of national economy	5	8.3
Affect the bank economy and trust to customer	18	30.0
Unemployment	1	1.7
Missing	2	3.3
Total	**60**	**100.0**

Source: Researchers (2013)

The analysis in Table 4.5 above show that 30 percent of the respondents argued that cybercrime affect the banking economy and reduces trust to customers and 21.7 percent said that it contributing to loss of revenues.

Figure 4.5: Show the Law That Governing Cybercrime (N=60)



Source: Researchers (2013)

The analysis in Figure 4.5 and Figure 4.5 above show that 56.7 percent of the respondents said that no cyber law while 43.3 percent said that there is cyber law.

4.6 Measures toward cybercrime

In the objective of the study that aimed to identify measures taken by the government to fight against the increase of cybercrime in Tanzania mainland. The analysis in Table 4.6 shows that a total of 36 respondents (60%) know the necessary skills and knowledge required to curb cybercrime while 24 of the respondents (40%) argued that, they do not know the skills and knowledge required.

Table 4.6: Factors relating to Cybercrime (N=60

Response	Yes	No	Percent
Cybercrime trends	9(15%)	51(85%)	100.0
Awareness of cybercrime	9(15%)	50(83.3%)	98.3
Obstacles facing investigation	8(13.3%)	52(86.7%)	100.0
Skills/Knowledge	36(60%)	24(40%)	100.0
Is there any cyber law	26(43.3%)	34(56.7%)	100.0

Source: Researchers (2013)

The analysis in Table 4.6 shows that a total of 30 respondents (50%) argued that computer skill or knowledge is important in solving the problems of cybercrime, 16 of respondents (26.7%) said they need investigative skills or knowledge, said they need financial skill or knowledge while and 5 respondents (8.5%) they need electronic skill or knowledge.

Table 4.6: Show Skills or Knowledge toward Cybercrime (N=60)

	Response	Frequency	Valid Percent
Knowledge and skills needed to curb cybercrime	investigation skills	16	26.7
	computer skills	30	50.0
	electronic skills	5	8.3
	legal knowledge	1	1.7
	financial	8	13.3
	Total	**60**	**100.0**

Source: Researchers (2013)

The shown in Table 4.6 above indicate that 86.7 percent said that, no obstacles facing the investigation officers of cybercrime whereby 13.3 percent argued for, that there is an obstacle for investigation officer of computer related crime. The analysis in Table 4.6 below; showed that 46 percent of respondents argued that lack of experience of modern technology usage in investigation, 45 said inadequate of experience of evidence extraction, while 8.3 percent said evidence contamination are the main obstacles that faced the investigation officers of cybercrime.

Table 4.6: Show Obstacles towards Cybercrime (N=60)

Obstacles facing investigation officer	Frequency	Valid Percent
inadequate experience on evidence extraction	27	45.0
evidence contamination	5	8.3
lack of experience on modern technology usage in investigation	28	46.7
Total	**60**	**100.0**

Source: Researchers (2013)

Table 4.6 shows different measures taken by the Government of Tanzania to curb cybercrime, the measures includes; capacity building and public awareness creation, establishment of cybercrime unit in the department of Police, International collaboration in controlling cybercrime, the use of CCTV camera in ATM,

preparation of cybercrime bills of law and find better software to detect intruders and establishment of financial intelligence, fraud and property financial crime unit.

Table 4.6: Show the Measures towards Cybercrime (N=60)

Measures taken to fight against cybercrime	Frequency	Percent
Capacity building and public awareness creation	16	26.7
International collaboration in controlling cybercrime	8	13.3
Procumbent of modern forensic equipment	2	3.3
Establishment of cybercrime unit	15	25.0
Preparing cybercrime bill of law	6	10.0
Establishment of financial intelligence, fraud and property financial crime unit	3	5.0
the use of CCTV camera in the ATM machine	7	11.7
find better software to detect intruders	3	5.0
Total	**60**	**100.0**

Source: Researchers (2013)

Table 4.6: Show Reasons for Obstacles Facing Investigation Officer

	Frequency	Percent
No cybercrime law	24	40.0
Lack of knowledge on ICT	5	8.3
Inadequate tools for computer investigation	6	10.0
Inadequate forensic computer investigative skills	9	15.0
Lack of knowledge on advanced technology	10	16.7
Inadequate training	6	10.0
Total	**60**	**100.0**

Source: Researchers (2013)

The findings in Table 4.6 present the reasons for the obstacles facing investigation officer, 40 percent of the respondent argued that is due to lack of cybercrime law, 16.7 percent said lack of knowledge on advanced technology, 15 percent inadequate

forensic computer investigative skills, 10 percent inadequate tools for computer investigation and inadequate training while 8.3 percent lack of knowledge on ICT.

The findings in Table 4.6 presents the cross tabulation between the effect of cybercrime and the factors accelerating the trend of cybercrime in Tanzania Mainland. The results shows that there are statistically significant association between trends of cybercrime (p=0.006), increased trend of cybercrime (p=0.032). While, there are no statistically association between effect of cybercrime and awareness.

Table 4.6: Cross Tabulation between Effect of Cybercrime and Factors Accelerating the Trend of Cybercrime.

Factors	**are aware of the cybercrime**				**factors accelerating the trend of cybercrime**			
	Yes	No	%	Fisher's exact P-value	yes	no	%	Fisher's exact P-value
Theft and money	16.7%	83.3%	100.0	0.032	8.3%	91.7%	100	0.006
	25%	75%	100.0		7.7%	92.3%	100	
Loss of revenue	20%	80%	100.0		20.0%	80.0%	100	
Destabilization					11.1%	88.9%	100	
of national economy	16.7%	83.3%	100.0					
Affect the bank economy and trust to customer								

Source: Researchers (2013)

CHAPTER FIVE

DISCUSSION OF THE FINDINGS

5.1 Introduction

The study conducted focused on cybercrime and criminal investigation: The challenges within the Tanzania Police Force, a case of Tanzania Police Force Head quarters. The three key objectives were used include: to identify factors accelerating the trend of cybercrime, to identify the effects of cybercrime and to identify measures taken by the Tanzania Government to fight against the increase of cybercrime in Tanzania mainland.

5.2 Factors accelerating the trend of cybercrime

Then survey in 4.4 shows that, new technology, electron banking system and internet banking; financial gain; insufficient technology capabilities, electronic storage of valuable information, unemployment and immigrant of foreigners with knowledge of ICT are the factors that accelerating the trend of cybercrime. The findings concur with the results of Olowo (2009, Paganinip (2012) and later results obtained by Triphy and Mishra (2013), who attest that advanced in technology will continue to provide criminals the tools to facilitate the commission of traditional crime.

Noted earlier in 4.4 the results show that electronic banking system and internet banking are among the factor accelerating the trend of cybercrime in Tanzania mainland. This is consistency with the results of Tripathy and Mishra (2013) who attested that one of the major rises of identity fraud was due to increased internet transition or online banking and electronic financial transaction. Similar, in the results of Njoroge (2012) who indicated that the diverse product lines and mobile banking solutions open up financial serious organisation increased cybercrime.

As indicated in 4.4 the findings show that financial gain accelerated the trends of cybercrime in Tanzania mainland. This concurs with the results of Longe and Chimeke (2008) and later the results obtained by Panda et al (2012)4 who attested that, organised crime groups are using the internet for major fraud and theft to earn millions per year leading to loss to investors, who confirmed that offline criminal have gone high-Tech and are making huge money. Similarly, it was noted that, cybercriminal are likely to participate in deviant behaviour because they want immediate gratification as discussed in the self-control theory propounded by Travis Hirschi and Michael Gottfredson in 1990 and published in A General Theory of Crime (Gzsybrowsk 2012). This is contrary to the results of Olowo (2009) who argued that the trend of cybercrime is motivated by fraud, this was revealed with the increase of counterfeiting due application of computer in daily activities Paganinip (2012) which led to identity frauds as the results of inadequate security (Gregor and Kroner, 2006). In my view illegal immigration and the mobility of international migration also accelerated the trends of cybercrime. This concurred with the results of Paganinip (2012) who attested that cybercrime can be due to increased international migration mobility of individual and families.

As shown in 4.4 insufficient technological knowledge and unawareness to ICT for user contributed to trend of cybercrime in Tanzania mainland. This is consistent with the results of Kwak, et al. (2005), Methew (2012), Tanzania Police Annual Crime Report, (2012) and later results obtained by Mehta & Singh (2013) who demonstrated that lack of awareness and low level of internet security making an important heaven for cybercriminal. Similarly, as noted earlier in the results of Danquah et al., (2012) and later results obtained by Wada & Odulaja, (2012) who indicated that lack of knowledge and limited awareness on the technology contribute to cybercrime in Tanzania mainland. To update lack of confidentiality and trust to both in private and public sector can attribute to the trends of cybercrime in Tanzania Mainland as noted earlier in the results of ASLAM (2006) who attested that internet user are not

[4] Panda et al (2012) Cybercrime and their Impacts: A Review; International Journal of Engineering Research and Application (IJERA), ISSN: 2248-9622, Vol. 2, Issue, Mar-Apr 2012, Available online at www.ijera.com. Accessed on 26/07/2012

shopping online due to lack of trust and fear over personal security and lack of trust companies over the internet.

As noted earlier in 4.4 the research findings show that the trends of cybercrime is accelerated with the lack of cybercrime law in Tanzania mainland. This consistent with the results of Ally (2011) who indicated that we need cyber law to criminalize the sabotage, hackers and crater and later the results obtained by Telecommunication Development Center (2012) which attested that deterring cybercrime is an integral component of national cyber security and critical information infrastructure protection strategy including adoption of appropriate legislation against misuse of ICTs for criminal and activities intended to affect the integrity of national critical infrastructure.

The study in 4.4 tells us that Lack of cybercrime as the control mechanism in cybercrime in Tanzania mainland was identified as the factor accelerating the trends of crime. This is consistent with the results of Liganga (2012) and later in the results of Pratt and Cullen (2000), who attested that lack of self control is a strong predictor of involvement in cybercriminal. Therefore, in order to teach the community self-control, someone must monitor behaviour, recognize deviant, and punish behaviour, (Gzsybrowsk 2012). This is consistent with the result of Wada and Odulaja (2012) attested that, the response of technology to cybercrime problems centre on the use of computer security theories to design and evolve solution that provides authentication verification, non-repudiations and models rely on the use of cryptography, steganography, network protocols, and the use of software engineering process models to develop systems that offer some forum of protection for users and the information infrastructure. Furthermore cybercrime thrives on the web today because the internet did not inculcate in the protocols from the onset a mechanism theft allows a host to selectively refuse message. Contrary to the results of Pratt and Cullen (2000), in their study, they found that lack of self control is a strong predictor of involvement in cybercriminal.

In my opinion, there is no cyber law in Tanzania that regulates the use of ICT particularly the internet and electronic money transfer, the use of digital tools, online transaction of money and online business, therefore the government required to enact cyber law as one of the measures in order to control the illegal online activities of cybercrime.

To conclude, the Government of Tanzania should develop stronger cyber security system to protect the public and private sector from being victim of the new technology. This concurred with the results of Telecommunication Development Center (2012)5 which indicated the needs of development of technical protection system to prevent citizens from becoming victims of cybercrime where. Contrary the result of Kalunde (2011) who attested that cybercriminal occurs in countries that has inadequate cyber laws6.

Also the Government of Tanzania mainland should make use of multidisciplinary approaches in combating cybercrime, as Legal, Technical and procedures measures to promote adoption of enhanced technique to improve security, organisation structures centred on prevention, detection, response to and crisis management of cyber attacks and capacity buildings to address national policy agenda and international dialogue in dealing with cybercrime.

5.3 Effects of cybercrime

The researchers' findings in 4.5 indicated that, cybercrime had affected the banking sector economic and loss trust to customer. This concur with the results of Curtis and Gordon (2000), FBI Computer Crime Security (2005), Guardian reporter (2013)7, Tanzania Daily news (2013), and later the results attained from "Mwananchi" Local New (2013) which demonstrated that theft of 500millions and 194 NMB and Diamond Trust Bank ATM card, 36 KCB ATM cards and other 18 ATM cards with no logo and equipment to manufacture fake ATM cards in Mwanza city, 20 million at

[5] Telecommunication Development Centre, 2012.
[6] Kalunde (2011) The Status of Cybercrime in Tanzania; Presented at Octopus Conference on Cooperation Against Cybercrime, 10th Anniversary of the Budapest Convention; Strasbourg, France.
[7] TCRA, Police wade war on cybercrime, February 8, 2013 by Guardian correspondent – Morogoro.

Tukuyu NMB8 which make Tanzania Banks lose over 80billions to cybercrime9. Similar, it was reported in "Mwananchi" Local New that Tanzania lost 892.18billion on cybercrime last financial.

As noted earlier in 4.5 identities theft is among the identified effect accelerated the trend of cybercrime in Tanzania mainland. This triangulated with the results of Salifu (2008) and later the results achieve by Fraud trend (2010) which attested that theft of cards information by using a small electronic device (skimmer) to swipe and store victim's credit and debit card number whereby the perpetrator accomplish this by placing the device over the ATM card slot and using a hidden camera to read PINS.

In my view due to the effects of cybercrime to customer poses another challenge which results to lose confidence on application of modern technology in activities through electronic and internet banking transfer. This is consistent with the result of Panda et al (2012) reports sponsored by the Butter Business Bureau Online; indicate that over 75 percent of online shoppers terminate an online transaction. Similar, in Fraud trend (2010) which indicated approximately 60 percent of bank frauds cases where data breach or theft of funds are due worker of the insider. Unfortunately, employees and contractors who access financial institutional systems during course of work know the system better than anyone else and they are better poisoned to exploit the systems.

The research finding in 4.5 shows that theft and money Laundering was due to uncontrolled cybercrime in Tanzania mainland. The findings concur with the results of (2009) and later results obtained by Fraud trends of (2010) who attest that Money-Laundering is a unique opportunity of quick development of financial infrastructure allowing transfer of momentary fund to any state and electronic transfer is a tool of concealing source of money intakes and laundering illegally earned money.

[8] Chawe Merali (27 February 2013). Tanzania Four Nobbed over 20millions ATM Theft; Tanzania Daily News (DSM)

[9] Tanzania Daily news reported on Tuesday July 27, 2013. Banks Lose over 80billion to cybercrime Pg

In my view majority of people who own bank account in foreign country, run big estate and large scale industries in Tanzania and outside Tanzania mighty be involving in Money Laundering. This concur with the result by Fraud trend (2010) which indicate that they transfer money into foreign bank accounts, investing in large-scale brick-and-mortar enterprises to hide their ill-gotten gains examples buying restaurants, or developing real estate. It is reported Gonzalez was really to purchase equity in a Miami night club before his arrest.10

In conclusion, combating cybercrime needs Government commitment in addressing the problems at hand and investing in computer engineering skills and forensic computer investigation together with enacting cyber law and capacity building and awareness creation to the user. In this study, the research finding reveals that cybercrime to destabilisation of the national economic. This concur with the results of Curtis and Gordon (2000), Ipu et al (2011) and afterwards results obtained by Mwananchi (2013) which attested that, destabilization of the national economy and financial loss and continue to affect the national security.

Panda et al (2012)11 organised crime groups are using the internet for major fraud and theft activities. The trends indicating organised crime involvement in white collar crime. Interne based stock fraud has earned criminals millions per year leading to loss to investors, The Norton Cybercrime disclosed that over 74million people were victim of cybercrime in 2010. The criminal act as resulted in direct financial losses. Some survey indicated that 80 percent of companies' survey acknowledged financial losses due to computer breaches.

The analysis in 4.6 revealed that, Lack of experience of modern technology usage in investigation, inadequate of experience of evidence extraction and evidence contamination are obstacles facing the investigation officers of cybercrime as by the

[10] Fraud trends in 2010. Top Threats From a Growing Underground Economic , First Data white Paper
[11] Panda et al (2012) Cybercrime and their Impacts: A Review; International Journal of Engineering Research and Application (IJERA), ISSN: 2248-9622, Vol. 2, Issue, Mar-Apr 2012, Available online at www.ijera.com. Accessed on 26/07/2012

journal knowledge empower Africa that "lack of credible evidence due to poor investigation techniques coupled with a limited forensic capacity" (Robison, 2009).

5.4 Measures against the increase of cybercrime in Tanzania

The research findings in 4.6 illustrated that capacity building and public awareness, was one among the measures adopted to fight against cybercrime in Tanzania mainland. This finding concur with the results of Broadhurst and Roderic (2006) who indicated that improve security awareness by providing adequate resources to secure transactions and equip system operators and administrators. Another findings of the study revealed that establishment of cybercrime unit in the department of Tanzania Police Force is indeed a new step forward in combating cybercrime. This is consistency with the results of Ally, (2011) who attested that cybercrime can be tackled through impelling coordinated law enforcement and harmonization policy that deals with confidentiality and security of processing personal data against cybercrime. Similarly, the results of Broadhurst and Roderic (2006) who demonstrated that combating cybercrime takes steps to ensure that technology does not outpace the ability of law enforcement to investigate and enact substantive and procedural law adequate to cope with current anticipated manifestation of cybercrime and development of forensic computing skills by law enforcement and investigative skills personnel and mechanisms for operational.

As noted earlier in the study findings in 4.6, that, international collaboration was ranked, as the measures in combating cybercrime in Tanzania mainland. This concurred with the results of Broadhurst and Roderic (2006) who attested that strengthening of international initiatives by updating the existing treaties and agreements to recognise the existence threats and transnational nature of high-tech computer crime and strive for legal harmonization. This is consistent with the arguments that, Government needs to coordinate activity and promoting public confidence in the safety and security of the internet in collaboration with international

partners to tackle the problem collectively against cybercrime12. And later in the results of (Gzsybrowsk, 2012) who demonstrate that no society can afford to accuse criminal matters without duly accepting its responsibilities.

Additionally, it was noted earlier in the findings in 4.6 that, the uses of CCTV camera in banking is another measures aimed to fight hand in hand with the fuelled rate of cybercrime. This concurs with the result of Danquah, et al (2012) who attested that the use of automated access control system and surveillance camera can serve as deterrents because they increased the perceived risk of being apprehended. Theory explains more the process of criminal and the decision to commit crime which is a problem to cyber. Contrary, the installation of the CCTV camera in most of banking system and ATM has not break the cybercriminal intention to clone customer's data and access their financial information and went free.

In conclusion, the measures considered in attempting fighting against cybercrime in Tanzania are not fully implemented and the ICT policy is not well enhanced the community understand the effects caused by cybercrime in the country. Therefore Tanzania needs to sign and implements different international treaties of cybercrime and enacting cybercrime law to fight against the cybercrime, capacity building and training of the community on the application and the impact of new technology in daily applications.

[12] Global project on cybercrime; available at www.coe.int/cybercrime: version 14, October 2011, Strasbourg, France. Draft/work in progress cybercrime strategies.

CHAPTER SIX

SUMMARY, CONCLUSIONS AND POLICY IMPLICATIONS

6.1 Introduction

This chapter briefly concludes the overall findings on Cybercrime and Criminal Investigation: The challenges within the Tanzania Police Force Forensic Laboratory. The chapter includes summary, conclusion and policy implication. The part includes conclusion in line with the research questions, objectives and the results from the study.

6.2 Summary

The introduction of Information and Communication Technology to Tanzania mainland has many challenges, which must be addressed by the government, international agents and other development partners. The main concerns of Tanzanians are how to protect citizen from the impact of cybercrime due to lack of knowledge and limit awareness on new technology. However the current law do not protect consumers against the risk involved online transaction, electronic money transfer, and online business transaction. Therefore the Government of Tanzania should enact cyber law that addresses the challenges of ICT policy and shortage of knowledge and skilled personnel to resolve the problem of cybercrime.

This study used qualitative and quantitative approaches, which aimed to investigate Cybercrime and Criminal investigation: The challenges within Tanzania Police Force Forensic Laboratory. The study used both secondary and primary sources of data collected from selected banking institution in Ilala Municipality, in Dar es Salaam. A total of 60 respondent, twenty cybercrime officer, ten NMB officers, ten CRDB officers, ten TPB officers and ten TCRA officers were interviewed. The SPSS version 16.0 software was used to analysis the primary data collected from Ilala District, Dar es Salaam.

Majority of the respondents revealed that, new technology; electron banking system and internet banking; financial gain, insufficient technology capabilities, electronic storage of valuable information, unemployment and immigrant of foreigners with knowledge of ICT are the challenges facing the Tanzania Police Force Criminal Investigation Machinery on the hand side they are cybercrime accelerating factors. The finding indicates that advanced in technology seemed to provide criminals with tools to facilitate the commission crime. Additionally, it had resulted that there were low level of understanding on the application of knowledge of ICT, the findings reavelled that lack of awareness, low level of internet security and absence of cyber law has threatened the the user. Furthermore, majority of the citizen are unaware about the cybercrimes, are the result they even not protecting their pin number of their ATM card.

However, findings indicated that cybercrime effects includes, theft, money laundering, loss of fund, increased white collar crime, cyber harassment, loss of government revenue, deterioration of the national economy, affect the banking sector economy, mistrust to customer. Cybercrime cause economical imbalances and price skyrocket, social trauma, exploitation of victims, political instability and promotes financial crime through internets and mobile phone.

The analysis revealed that, the challenges facing the criminal investigation is due lack of experience on the use of modern technology in investigation of cybercrimes, inadequate of experience of evidence extraction and evidence this may results to lack of credible evidence. Apart from the establishment of cybercrime unit, the Government should focus on capacity building, public awareness, and foster International collaboration and enactment of new law that will deter the increased trends of modern crime to Tanzania mainland.

6.3 Conclusion

Therefore, the Government should make sure that capacity building and public aware to citizen will contributes and institutional awareness to decreased trends of cybercrime. We found that advancement in new technology contributed to application

of ICT in our daily activities, which in turn it became a free zone for cybercriminal. Our data suggests that the government should provide education on application of ICT, knowledge and skill empowerment to cybercrime investigator. Finally, the Government should enact cyber law as one of the measures to control the illegal online activities. Also investing in new technology in order to ensure safety application to ICT in officials' purpose, daily activities like banking by use of electronic money transaction such as M- Pesa, Tigo- Pesa and ATM, and provision community mass education concerned usage of new technology.

6.4 Policy Implications

If the Government of Tanzania mainland failed to develop stronger cyber security systems to protect the public and private sector from technological victimizations, then the trend of cybercrime activity would increase and threaten the national security such as e-Government, e-business, e-trade and e-shopping which in turns led to low revenues. This cannot be achieved without Government commitment in addressing the problems and investing in computer engineering skills and forensic computer investigation together with enacting cyber law and capacity building and awareness creation to the user. Failure to plan, cybercrime can cause destabilization of the national economy and financial loss and continue to affect the national security.

If the ICT policy is implemented and the community is well educated on the application of new technology, then the trends of cybercrime and its effects to the community and businesses company may be reduced. Therefore Tanzania needs to sign and implements different international treaties of cybercrime and enacting cybercrime law to fight against the cybercrime, capacity building and training of the community on the application and the impact of new technology in daily applications. Information Communication and Technology awareness is crucial for combating cybercrime and reducing of online attack. Therefore the Government should provide strongly ICT security awareness training to users, employees and law enforcers to understand the risks and prevent. If the government fails to combat cybercrime then, the trend of cybercrime would affect the national developments in information communication technological.

6.5 Areas for Further Researches.

This study was conducted only in Ilala District, Dar es Salaam Region. It is hereby recommended that, the study be conducted in other district of Dar es Salaam or other areas in Tanzania to confirm the finding. More research should be done as:

(i) It is suggested that further research should be done on mobile phone money transfer because the study has shown some constraints on accessing cybercrime informations regarding their customers.

(ii) It is suggested that further research should be done to investigate the effectiveness of internet service providers in fighting against cybercrime.

(iii) It is suggested that further research should be done to investigate the effectiveness of the policy in creating awareness to the community about the application of ICT.

(iv) It is suggested that further research should be done investigate if the Government has provide strongly ICT security on e-Government, e-business, e-trade and e-shopping.

REFERENCES

Aaker at el. (2002). *Marketing Research* (7th ed); New Delhi. John Wiley & Son, Inc.

Adam and Kamuzora. (2008). *Research Methods for Business and Social Studies*; Dar es Salaam, Tanzania; Mzumbe Book Project.

Ally, A. (2011). *The Impact of ICT Revolution in Tanzania's Legal System: A critical Analysis of Cybercrime and Computer Forensic Evidence*. Retrieved March 2013

ASLAM, D. M. (2006). Global Nature of Computer Crimes and the Convention on cybercrime. *volume 3, No. 2*, pp. 129-142. Winter. Retrieved February 4, 2013, from http://dergiler.ankara.edu.tr/dergiler/64/1541/16889

Athumani, R. (2012, August 22). Tanzania: War Against Cybercrime Stepped Up. *Tanzania Daily News*. doi:20120820128.hotmail centre, I. c. (2010, March 16). *Cybercrime losses double*. Retrieved February 05, 2013, from Google.

Barnes, D. (2001). *Research methods for empirical investigation on the process of formation of the operation strategy*: *International Journal of Operation and Production Management, Vol.21*

Business Software Alliance, (2007). *To fight from cyberspace: High tech and Law enforcement Expert on Defeating Today's cyber criminal*. Retrieved from World Wide Website.

Buzzell et al. (2006). Explaining use of online pornography: A test of self-control theory andopportunities for deviance. *Journal of Criminal Justice and Popular Culture*, *13*(2), 96-116. Retrieved December 27, 2011, from http://www.albany.edu/scj/jcjpc/vol13is2/Buzzell.pdf

Clough, J. (2010). *Principle of Cybercrime.* New York: United State of America of Cambridge University Press.

Cullen & Agnew. (2006). *Criminological theory: past to present essential readings*. (3rd ed., pp. 5-8). New York, NY: Oxford University Press.

Curtis et al. (2000). *A member of the Lexis - Nexis Risk Solutions Group.* The National Fraud Center, Inc.

Danquah and Longe. (n.d.). An Empirical Test Of The Space Transition Theory of Cyber Criminality: A case of Ghana and Beyond. *African Journa of Informationa and Communication Technologies, Volume.4*, 37-48.

Danquah et al. (2012l). Action speaks Lounder than Words- Understanding Cyber criminal Behavior Using Criminological Theories. *Journal of Internet Banking and Commerce*, *12*(1), 1-11. Retrieved February 7, 2013, from http://www.arraydev.com

Dror and Charlton (2006). Why Expert Make Error; Institute of Cognitive and Neuroscience University College London, London, United Kingdom; Journal of Forensic Identification 600-56(4).

Goodman, M. (1997). *Why Police Don't Care About Computer Crime*. (H. J. TECH, Producer) Retrieved February 08, 2013, from World Wide Website: http://www.tech360magazine.com

Gottfredson and Hirsh (1990). A general Theory of Crime; Stanford; Stanford University Press.

Gregor Urbas & Tony Krone. (2006, November). Mobile and Wireless technologies: Security and risk factor. *Trends and Issue in crime and criminology*(329).

Grzybowski (2012). An Examinationation of Cybercrime and Cybercrime Research; Self- control and Routine Activity Theory; Arisona; Arisona University

Hassan, A. (2009). *Role of Information and Communication Technology (ICT) in Enhancing the Livelihood of the Rural Poor.* UNDP, Tanzania. Dar es Salaam: Economic and Social Research Foundation TAKNET Policy Brief.

International Telecommunication Union, (2009). *Understanding Cybercrime*: A guide for ICT Application and Cybersecurity Division Policies and Strategies Department. (*International Telecommunication Union Cybercrime Legislation Reviews.*

Interpol. (2012, March 30). *Cybercrime*. Retrieved February 5, 2013, from http://www.interpol

Ipu, C.J*, et al,*. (2011). Effect of Cybercrime on State Security: Type, Impact and Mitigations with the Fibre Optic Deployment in Kenya. *Journal of information Assurance and Cybersecurity, 2011*, 20. doi:10.5171/2011.618585

Klerk P and Kop M. (2008). Societal Trends and Crime relevant factors. *An Overview for Dutch National Threat Assessment on Organised Crime 2008-2012*.

Kombo, K and Tromp, A.(2006). *Proposal and thesis writing*. Pauline Publications Africa. Nairobi.

Kothari, C.R (2003) Research Methodology; Methods and Technologies; New Delhi, Wishw, A Prakashen. 1116.

Kothari, C.R. (2004). *Research methodology: methods and techniques*; 2nd Ed. New Age international (P) LTD, India.

Kwak,C., Robinson, T., and Kwak, D. (2005). *Handbook for Transnational Crime and Jstice.* SAGE Publication, Inc, doi.

Liganga, F. (2012). *An Assessmentof Legal System in Relation to the Increasing rate of cybercrime in Tanzania.* Dissertation, Dar es Salaam. Retrieved March 2013

Longe, O.B and Chiemeke, S.C. (2008). Cybercrime and Criminality in Nigeria - What Role are Internet Access Point in Playing? *European Journal of Social Science, Volume, 6*, 132-139.

Majaliwa, C. (2011, May 23). *Tanzania Police to Step up war on Cybercrime*. Retrieved February 8, 2013 , from Tanzania Daily News: http://in2eastafrica.net

Makinde et al. (2012, August). Cybercrime in Nigeria Causes, Effects and the Way Out. *ARPN Journal of Science and technology, 2*(7). Retrieved February 7, 2013, from http:www.ejournalofscience.org

Mehta and. Singh (2013). A Study of Awareness About Cybercrime law In Indian Society. *International Journal of Computers and Business Research (IJCBR).*

Methew, M. (2012, January 12). Law Against Cybercrime Coming. Tanzania *Daily News*. doi:913.

Milhon, T. (2007). *Cybercrime How to Avoid Becoming a Victim by- Tre crime.*

Mirondo, R. (2010, November 16). *East African Police Personnel train on new forensic skills*. doi:4/5582.

Mwita, S (2012, July 26). *Cybercrime Warrisome*. Retrieved February 12, 2013, from World Wide Website: http://www.allafrican.com

Nir Kshetri. (2010). *Diffusion of Effect of Cybercrime in Developing Economies.* USA;1057-1079.

Olowo, D. (2009). Cybercrime and Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa. *Journal of Information, Law and Technology (JILT)*, 1-8.

Osborne et al. (2008). 55 Trends Now Shaping the future of policing. *The proteus Trend series, 1*(1).

Outlaw (2001). *A Routine Activity Approach to the Study of intimate partner violence;* A Thesis in crime, Law, and Justice; Unpublished doctor of philosophy.

Pack, W. (2012/2013). The South Africa Cybercrime threat Barometer. *A Strategic Public- Private Pertnership Initiative to Combat Cybercrimemin SA, 2012/2013.* Retrieved February 05, 2013, from www.wolfpack risk.com.

Paganinip. (2012, April 23). *Analysis of Cybercrime and its impacts on private and military Sectors.* doi:4631

Panda et al (2012) Cybercrime and their Impacts: A Review; *International Journal of Engineering Research and Application (IJERA), ISSN: 2248-9622, Vol. 2,* Issue, Mar-Apr 2012, Available online at www.ijera.com. Accessed on 26/07/2012

Pant et al. (2012). Forensic Computing-Technology to Combat Cybercrime. *International Journal of Advanced Research in Computer Science and Software Engineering*, 301-304.

Pratt and Cullen (2000). The empirical status of Gottfredson and Hirsch's *general theory of crime: A meta-analysis.* Criminology, 38, 931-964.

Proffesor, S. (2010, November 5). Shortage of Skilled Officer. *Australian Cybercrime Investigation*.

Robins, S. (2009, October). Policy Brief: Addressing the Challenges of enforcement in African. *Journal Knowledge empowers African, Nr, 16*. Retrieved from Http://www.issafrican.org.

Roderic, B. (2006). Development in the global Law enforcement of cybercrime. *Policing: An Internation Journal of Police strategiies and Mangement, 29*(3), 408-433. doi:1o.1108/1363951061068684674

Salifu, A. (2008). The Impact of internet Crime on development. *Journal of Financial Crime, 15*(4), 432-443. doi:10.1108/13590790810907254

Schell, B.H and Clemens, M. (2004). *Cybercrime: A Reference Handbook.* ABC - CLIO.

Schnierer and Vivian. (2010). *Factors affecting Crime rate in Indigenous Community in NSW: a pilot study in Bourke and Lightinig Ridge*. Jumbunne Indigenous House Learning.

Tanzania Police Force (2011). *Annual Crime report.* Laboratory. Dar es Salaam.

Tanzania Police Force (2012). *Annual Crime report.* Laboratory. Dar es Salaam.

Tripathy and Mishra (2013). Protective Measures in e-Commerce to deal with Security Threat Arising Out of Social Issues - A framework. *International Journal of Computer Engineering and Technology, Vol.4*, 46-53.

Wada, F. and Odulaja, G.O. (2012, january). Assessing Cybercrimeand its Impact on E-Banking in Nigeria Using Social Theories. *African Journal of Comouter and Information Communication and Technolg*, 69-82.

APPENDICES

Appendix 1: Questionnaire for cybercrime officer

The question has been prepared for the purpose of collecting information that help to accomplish a research titled "Cybercrime and Criminal Investigation: the challenges within Tanzania Police Force Forensic Laboratory". This study as well, is done as a partial fulfilment of the requirements for the Award of the Degree of Master in Public Administration (MPA). All the answer to the question will be kept confidential, and will never be used for different purpose other than academic purposes. Thanks for accepting and spent your precious time to answer these questions. Questionnaire to Cybercrime, CRDB, NMB, TPB and TCRA officials

PERSONA PARTICULARS

Please tick the appropriate box provided to each question below

1	What is your gender?	Male{] Female [ ]
2	What is your age range?	Below 18-28 [ ] 28-38 [ ] 38-48 [ ] 48-58 [ ] 58-68 [ ]
4	What departmental unit are you working for?	
5	What level are you holding?	Senior Management[ ] Junior level management [ ]
5	How long have you been working in your departmental unit?	Less than 5yrs [ ] 5-10yrs [ ] 11-15yrs [ ] 16-20yrs [ ] Over 20yrs [ ]
7	In your experience do you know the factors accelerating the trend of cybercrime?	Yes [ ] No [ ]
8	Give reasons for your answers in 7 above	
9	Does the trend of cybercrime decreasing in Tanzania Mainland?	Yes [ ] No [ ]

10	Give reasons	
11	Are you aware of the cybercrime?	Yes [ ] No [ ]
12	If yes what are effects of cybercrime in Tanzania Mainland	
13	How is your organisation performing in the implementation of cyber-space security?	Very satisfactory [ ] Satisfactory [ ] Dissatisfactory [ ] Very Dissatisfied [ ]
14	Is there any obstacles facing the investigation officer of computer related crime in Tanzania Mainland?	Yes [ ] No [ ]
14	If the answer is yes in 13 above please mention them	
15	Do you know the required skills/knowledge needed to curb cybercrime?	Yes [ ] No [ ]
16	If the answer is YES in 15 above please what are they?	
17	Do you think the Investigation officers always have sufficient experience to extract evidence successfully?	Yes [ ] No [ ]
18	18 If the answer is NO in 17 above give reasons	
19	What are measures taken by Tanzania Police force to curb cybercrime in Tanzania Mainland	
20	Is there any policy, regulation or law which govern cybercrime in Tanzania Mainland?	Yes [ ] No [ ]
	Give reason for your answer in Qn 20 above	

Appendix 2: Questionnaire for NMB officer

The question has been prepared for the purpose of collecting information that help to accomplish a research titled "Cybercrime and Criminal Investigation: the challenges within Tanzania Police Force Forensic Laboratory". This study as well, is done as a partial fulfilment of the requirements for the Award of the Degree of Master in Public Administration (MPA). All the answer to the question will be kept confidential, and will never be used for different purpose other than academic purposes. Thanks for accepting and spent your precious time to answer these questions. Questionnaire to Cybercrime, CRDB, NMB, TPB and TCRA officials

PERSONA PARTICULARS

Please tick the appropriate box provided to each question below

1	What is your gender?	Male Female [ ] [ ]
2	What is your age range?	Below 18-28 [ ] 28-38 [ ] 38-48 [ ] 48-58 [ ] 58-68 [ ]
4	What departmental unit are you working for?	
5	What level are you holding?	Senior Management[ ] Junior level management [ ]
5	How long have you been working in your departmental unit?	Less than 5yrs [ ] 5-10yrs [ ] 11-15yrs [ ] 16-20yrs [ ] Over 20yrs [ ]
7	In your experience do you know the factors accelerating the trend of cybercrime?	Yes [ ] No [ ]
8	Give reasons for your answers in 7 above	
9	Does the trend of cybercrime decreasing in Tanzania Mainland?	Yes [ ] No [ ]

10	Give reasons	
11	Are you aware of the cybercrime?	Yes [ ] No [ ]
12	If yes what are effects of cybercrime in Tanzania Mainland	
13	How is your organisation performing in the implementation of cyber-space security?	Very satisfactory [ ] Satisfactory [ ] Dissatisfactory [ ] Very Dissatisfied [ ]
14	Is there any obstacles facing the investigation officer of computer related crime in Tanzania Mainland?	Yes [ ] No [ ]
14	If the answer is yes in 13 above please mention them	
15	Do you know the required skills/knowledge needed to curb cybercrime?	Yes [ ] No [ ]
16	If the answer is YES in 15 above please what are they?	
17	Do you think the Investigation officers always have sufficient experience to extract evidence successfully?	Yes [ ] No [ ]
18	18 If the answer is NO in 17 above give reasons	
19	What are measures taken by Tanzania Police force to curb cybercrime in Tanzania Mainland	
20	Is there any policy, regulation or law which govern cybercrime in Tanzania Mainland?	Yes [ ] No [ ]
	Give reason for your answer in Qn 20 above	

Appendix 3: Questionnaire for CRDB officer

The question has been prepared for the purpose of collecting information that help to accomplish a research titled "Cybercrime and Criminal Investigation: the challenges within Tanzania Police Force Forensic Laboratory". This study as well, is done as a partial fulfilment of the requirements for the Award of the Degree of Master in Public Administration (MPA). All the answer to the question will be kept confidential, and will never be used for different purpose other than academic purposes. Thanks for accepting and spent your precious time to answer these questions. Questionnaire to Cybercrime, CRDB, NMB, TPB and TCRA officials

PERSONA PARTICULARS

Please tick the appropriate box provided to each question below

1	What is your gender?	Male{] Female [ ]
2	What is your age range?	Below 18-28 [ ] 28-38 [ ] 38-48 [ ] 48-58 [ ] 58-68 [ ]
4	What departmental unit are you working for?	
5	What level are you holding?	Senior Management[ ] Junior level management [ ]
5	How long have you been working in your departmental unit?	Less than 5yrs [ ] 5-10yrs [ ] 11-15yrs [ ] 16-20yrs [ ] Over 20yrs [ ]
7	In your experience do you know the factors accelerating the trend of cybercrime?	Yes [ ] No [ ]
8	Give reasons for your answers in 7 above	
9	Does the trend of cybercrime decreasing in Tanzania Mainland?	Yes [ ] No [ ]
10	Give reasons	
11	Are you aware of the cybercrime?	Yes [ ] No [ ]

12	If yes what are effects of cybercrime in Tanzania Mainland	
13	How is your organisation performing in the implementation of cyber-space security?	Very satisfactory [ ] Satisfactory [ ] Dissatisfactory [ ] Very Dissatisfied [ ]
14	Is there any obstacles facing the investigation officer of computer related crime in Tanzania Mainland?	Yes [ ] No [ ]
14	If the answer is yes in 13 above please mention them	
15	Do you know the required skills/knowledge needed to curb cybercrime?	Yes [ ] No [ ]
16	If the answer is YES in 15 above please what are they?	
17	Do you think the Investigation officers always have sufficient experience to extract evidence successfully?	Yes [ ] No [ ]
18	18 If the answer is NO in 17 above give reasons	
19	What are measures taken by Tanzania Police force to curb cybercrime in Tanzania Mainland	
20	Is there any policy, regulation or law which govern cybercrime in Tanzania Mainland?	Yes [ ] No [ ]
	Give reason for your answer in Qn 20 above	

Appendix 4: Questionnaire for TPB officer

The question has been prepared for the purpose of collecting information that help to accomplish a research titled "Cybercrime and Criminal Investigation: the challenges within Tanzania Police Force Forensic Laboratory". This study as well, is done as a partial fulfilment of the requirements for the Award of the Degree of Master in Public Administration (MPA). All the answer to the question will be kept confidential, and will never be used for different purpose other than academic purposes. Thanks for accepting and spent your precious time to answer these questions. Questionnaire to Cybercrime, CRDB, NMB, TPB and TCRA officials

PERSONA PARTICULARS		
Please tick the appropriate box provided to each question below		
1	What is your gender?	Male{] Female [ ]
2	What is your age range?	Below 18-28 [ ] 28-38 [ ] 38-48 [ ] 48-58 [ ] 58-68 [ ]
4	What departmental unit are you working for?	
5	What level are you holding?	Senior Management[ ] Junior level management [ ]
5	How long have you been working in your departmental unit?	Less than 5yrs [ ] 5-10yrs [ ] 11-15yrs [ ] 16-20yrs [ ] Over 20yrs [ ]
7	In your experience do you know the factors accelerating the trend of cybercrime?	Yes [ ] No [ ]
8	Give reasons for your answers in 7 above	
9	Does the trend of cybercrime decreasing in Tanzania Mainland?	Yes [ ] No [ ]
10	Give reasons	

11	Are you aware of the cybercrime?	Yes [ ] No [ ]
12	If yes what are effects of cybercrime in Tanzania Mainland	
13	How is your organisation performing in the implementation of cyber-space security?	Very satisfactory [ ] Satisfactory [ ] Dissatisfactory [ ] Very Dissatisfied [ ]
14	Is there any obstacles facing the investigation officer of computer related crime in Tanzania Mainland?	Yes [ ] No [ ]
14	If the answer is yes in 13 above please mention them	
15	Do you know the required skills/knowledge needed to curb cybercrime?	Yes [ ] No [ ]
16	If the answer is YES in 15 above please what are they?	
17	Do you think the Investigation officers always have sufficient experience to extract evidence successfully?	Yes [ ] No [ ]
18	18 If the answer is NO in 17 above give reasons	
19	What are measures taken by Tanzania Police force to curb cybercrime in Tanzania Mainland	
20	Is there any policy, regulation or law which govern cybercrime in Tanzania Mainland? Give reason for your answer in Qn 20 above	Yes [ ] No [ ]

Appendix 5: Questionnaire for TCRA Officer

The question has been prepared for the purpose of collecting information that help to accomplish a research titled "Cybercrime and Criminal Investigation: the challenges within Tanzania Police Force Forensic Laboratory". This study as well, is done as a partial fulfilment of the requirements for the Award of the Degree of Master in Public Administration (MPA). All the answer to the question will be kept confidential, and will never be used for different purpose other than academic purposes. Thanks for accepting and spent your precious time to answer these questions. Questionnaire to Cybercrime, CRDB, NMB, TPB and TCRA officials

PERSONA PARTICULARS		
Please tick the appropriate box provided to each question below		
1	What is your gender?	Male{] Female [ ]
2	What is your age range?	Below 18-28 [ ] 28-38 [ ] 38-48 [ ] 48-58 [ ] 58-68 [ ]
4	What departmental unit are you working for?	
5	What level are you holding?	Senior Management[ ] Junior level management [ ]
5	How long have you been working in your departmental unit?	Less than 5yrs [ ] 5-10yrs [ ] 11-15yrs [ ] 16-20yrs [ ] Over 20yrs [ ]
7	In your experience do you know the factors accelerating the trend of cybercrime?	Yes [ ] No [ ]
8	Give reasons for your answers in 7 above	
9	Does the trend of cybercrime decreasing in Tanzania Mainland?	Yes [ ] No [ ]
10	Give reasons	
11	Are you aware of the cybercrime?	Yes [ ] No [ ]

12	If yes what are effects of cybercrime in Tanzania Mainland	
13	How is your organisation performing in the implementation of cyber-space security?	Very satisfactory [ ] Satisfactory [ ] Dissatisfactory [ ] Very Dissatisfied [ ]
14	Is there any obstacles facing the investigation officer of computer related crime in Tanzania Mainland?	Yes [ ] No [ ]
14	If the answer is yes in 13 above please mention them	
15	Do you know the required skills/knowledge needed to curb cybercrime?	Yes [ ] No [ ]
16	If the answer is YES in 15 above please what are they?	
17	Do you think the Investigation officers always have sufficient experience to extract evidence successfully?	Yes [ ] No [ ]
18	18 If the answer is NO in 17 above give reasons	
19	What are measures taken by Tanzania Police force to curb cybercrime in Tanzania Mainland	
20	Is there any policy, regulation or law which govern cybercrime in Tanzania Mainland?	Yes [ ] No [ ]
	Give reason for your answer in Qn 20 above	