CYBERCRIME AND THE LAW IN ZAMBIA

By

SIMUSOKWE LUPIYA

(25023179)

A dissertation submitted to the University of Zambia in partial fulfillment of the requirement of the degree of LL.B

THE UNIVERSITY OF ZAMBIA

LUSAKA

FEBRUARY 2009

I, **Chanda Nkoloma Tembo,** do hereby recommend that this Directed Research Essay prepared under my supervision by the said **Simusokwe Lupiya**, entitled:

CYBERCRIME AND THE LAW IN ZAMBIA

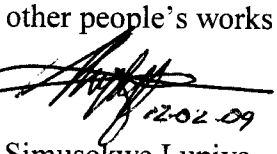
be accepted for Examination. I have checked it carefully and I am satisfied that it fulfills the requirements pertaining to the format as laid down in the regulations governing Obligatory Essays.

Mrs. **Chanda Nkoloma Tembo**, (LLB, LLM, AHCZ)

Supervisor **Date**15.03.09

COPYRIGHT DECLARATION

This dissertation represents my own work and that it has not been previously submitted for a degree at this or another University. I further declare that this work is duly mine and that where other people's works have been alluded to, due acknowledgements has thereto been made.



Simusokwe Lupiya

Email: lupiasimz2@yahoo.com

ABSTRACT

This paper argues that Zambia does not have a comprehensive legal structure to deter and prosecute cybercrime. It does this by examining international and national approaches to cybercrime, with a view to providing guidance for an effective framework capable of addressing this 'new' crime. Although the Computer Crimes and Misuse Act no 13 of 2004 now criminalises some cybercrimes, the Act still does not prohibit other major cybercrimes and this paper further argues that the Act imposes lighter sentences for offences that otherwise require hefty punishments. The paper further examines the relevant traditional legislation that may be used to combat cybercrime and advocates for appropriate legislative amendments that would take into account the present and possible future technological developments. The statistics of cybercrime in the country, it is argued, do not reflect the actual level of cyber criminality due to non reporting of such incidents and the essay advances ways that may ameliorate this unfortunate status. The paper also considers and examines the National ICT policy (2007) and Fifth National Development Plan (2006-2010) vis a vis government commitment in promoting safety on the electronic frontier especially that the development agenda in these documents advocate for increased use of ICT's. The guides for future reforms (legislative or otherwise) meant to address cybercrime concerns as depicted in the two policy documents are also highlighted. The paper also advocates for the adoption of an appropriate legal and regulatory framework especially in light of the fact that the attainment and sustenance of the MDG's is much dependent on reduced abuse of technology. The Cybercrime is a major global challenge requiring coordinated international effort. In a networked world no island is an island; cybercrime penetrates all countries because of its ability to cross national boundaries. In light of the above, this paper assesses the efforts at COMESA and SADC regional bodies and also recommends a model law that is based on the first international treaty which plays a key role in combating cybercrime while at the same time highlights the major concerns raised against the treaty. Furthermore, alive to the fact that criminal or penal sanctions can only be one element of the overall response to cybercrime, and that sanctions may not necessarily be the most efficient or desirable form of response, this paper, also discusses the viability of employing other ways of preventing or minimising the harm of cybercrime through means such as technological measures, regulatory controls and civil proceedings. Finally, it recognises that legislation alone cannot fight cybercrime; law enforcement must be equipped to implement the law, and private citizens must know about cybercrime.

DEDICATIONS

This dissertation is dedicated to the memory of my late beloved father, Mr. Stephen Lupiya Simusokwe (1957-1999).

ACKNOWLEDGEMENTS

This work is the result of extensive research and I would never have survived the research period, let alone produced this work, had it not been for the wonderful support and friendship of many people. Likewise, my success at University of Zambia has been supported by many people and in no particular order, I would like to thank the following:

My supervisor, Mrs. Nkoloma Tembo, for the insightful comments and valuable supervision throughout, steering me in the right direction, enriching my mind, and broadening my horizons.

To my best friend Suwilanji Nambela, for the love, care and support that kept me going through the best of times and the darkest of hours.

The Petro crew, Bwalya Mubanga, Wallace Chitungu, David Chakoleka, for the much valued and true friendship.

Changa Chitabo, Edgar Xhosa, Rex Zambwe,Valerie Kawangu, Hilda Mwanza and the rest of the fourth year class of 2008/9 for the friendship and for the big laughter that made classes worthwhile.

Darius Mangwatu, for being there for me especially when I much needed your friendship and company

My lovely mother, Mrs. Joyce M. Simusokwe for providing emotional support and, most important, love. Her care is flawless and I am forever grateful to her for being the best mother. My debt to her is beyond measure. I owe everything to her.

My mentor and uncle, Mr. Kalengo Njobvu for the much needed fatherly love and insightful guidance in all aspects of my life. His unfailing desire to see everyone do well is worth a great commendation.

My sincere and undeniable gratefulness go to my auntie, Mrs. Luhuna H. Njobvu, for her unyielding love and support. I am so grateful to her.

Uncle Samson Mwanza, for the encouragement, support and great sacrifices that he has endured for me. No words can ever express my thankfulness to him.

Our family, and particularly my brothers, sisters and counsins: Erick, Grace, Fanol, Michael, Kay, Stephen, Farae, Junior, Chiyeso and Kalengo, for all the support they have given to me. I am forever grateful to them.

I am solely responsible for this work and happy to

TABLE OF STATUTES

South Africa

Electronic Communications Transactions Act No.25 of 2002

Films and Publications Act 65 of 1996

United States of America

Can Spam Act of 2003

Delaware Code

Federal United States Code

Identity Theft Penalty Enhancement Act of 2004, HR, 1731

United Kingdom

Computer Crimes Act of 1990

Copyright, Designs and Patents Act of 1988

Criminal Justice and Public Order Act of 1994

Identity Cards Act of 2006

Protection of Children Act of 1978

Theft Act 1978 (as amended by the Theft Amendment Act (1996)

Sexual Offences Act of 2003

Zambia

Penal Code Act, Cap 87 of the Laws of Zambia

Computer Crimes and Misuse Act No.13 of 2004

Copyright and Performance Rights Act Cap 406 of the Laws of Zambia

TABLE OF CASES

Brinkibon v Stahag Stahl [1983] 2 AC 34.

CompuServe, Inc. v. Cyber Promotions, Inc. 962 [S.D. Ohio 1997].

Entores v Miles Far East Corp [1955] 2 QB 327

R v Absalon [1979] 68 Cr App R 183

TABLE OF CONTENTS

COPYRIGHT DECLARATION ii
ABSTRACT iii
DEDICATIONS iv
ACKNOWLEDGMENTS v
TABLE OF STATUTES vi
TABLES OF CASES vii
TABLE OF CONTENTS viii
LIST OF ACRONYMS x
WORKING DEFINITIONS xi

CHAPTER ONE : INTRODUCTION

1.0 General Introduction 1
1.1 Introduction 1
1.2 Problem Statement 2
1.3 Objectives of Study 3
1.4 Rationale and Justification 4
1.5 Research Questions 7
1.6 Methodology 7

CHAPTER TWO: A COMPARATIVE LAW ANALYSIS OF RESPONSES TO CYBERCRIME

2.0 Introduction 8
2.1 Challenges of cybercrime .....
2.2Comparative Law Analysis of Responses to Cybercrime
2.2.1 A brief background of cybercrime Legislation in Zambia 10
2.2.2 Unauthorised Access 11
2.2.3 Unauthorised Modification 12
2.2.4 Denial of Service Attacks 13
2.2.5 Unsolicited electronic mail (spam) 15
2.2.6 Unauthorised Interception 16
2.2.7 Pornography 17
2.2.8 Manufacture of devices furthering cybercrime 19
2.2.9 Computer Related Fraud 19
2.2.10 Computer Related Forgery 20
2.2.11 Infringement of Intellectual Property Rights 21
2.2.12 Theft 22
2.2.13 Inter-jurisdictional and Procedural Aspects 24
2.3 *E*-Commerce and the inadequacy of Traditional Legislation 25
2.4 Conclusion 27

CHAPTER THREE:

AN ASSESSMENT OF ZAMBIA'S POLICY MEASURES VIS A VIS CYBERCRIME

3.0 Introduction.....28
3.1 The National ICT Policy (2007)
3.1.0 Overview... 28
3.1.1 Developing the Legal and Regulatory framework (Policy goal number 12)...30
3.1.2 Promoting Security in the Information Society (Policy goal number 13).....31
3.2 The Fifth National Development Plan (2006-2010).....34
3.3 The Millennium Development Goals.....36
3.4 Conclusion.....37

CHAPTER FOUR:

A CASE FOR NON-PENAL MEASURES IN THE FIGHT AGAINST CYBERCRIME

4.0 Introduction.....38
4.1 An examination of formal statistics of cybercrime in Zambia.....38
4.2 The Employment of non-penal measures in the fight against cybercrime
4.2.0 Background.....40
4.2.1 Technological Measures.....41
4.2.2 Administrative Measures.....42
4.2.3 Civil Remedies.....44
4.3 Conclusion.....44

CHAPTER FIVE:

AN ASSESSMENT OF REGIONAL AND INTERNATIONAL EFFORTS

5.0 Introduction.....45
5.1 Regional Efforts
5.1.1 SADC.....45
5.1.2 COMESA.....46
5.2 International Efforts
5.2.1 United Nations 47
5.2.2 The G8.....47
5.2.3 INTERPOL 48
5.2.4 The Council of Europe Convention on Cybercrime
5.2.4.0 A Brief Overview 49
5.2.4.1 Potential Benefits of the Convention for Zambia.....49
5.2.4.2 Major concerns about the Convention.....50
5.3 Conclusion 52

CHAPTER SIX: RECOMMENDATIONS AND CONCLUSIONS

6.1 Conclusions 53
6.2 Recommendations 55

LIST OF ACRONYMS

CAZ -Communications Authority of Zambia

COMESA-Common Market for East and Southern Africa

FNDP -Fifth National Development Plan

ICT- Information and Communications Technology

INTERPOL- International Police

MDGs -Millennium Development Goals

SADC -Southern Africa Development Community

U.S –United States of America

U.K – United Kingdom

WORKING DEFINITIONS

Cybercrime- Criminal activity in which computers or networks are a tool, a target, or a place of criminal activity

Cyberspace- an indefinite place where individuals transact and communicate or simply an environment in which computer technology is central.

E-Commerce / Electronic Commerce – Business activities involving consumers, manufacturers, suppliers, service providers and intermediaries using computer networks such as the Internet.

E-Government service - means public service provided electronically by a ministry or Government Department, local authority, or body established by or under any law or controlled or funded by the Government.

Hacking- means gaining access to a computer system or network without permission

Information and Communication Technologies (ICT's) – Is a generic term used to express the convergence of information technology, broadcasting and communications. One prominent example is the Internet.

Information Technology (IT) – Embraces the use of computers, telecommunications and office systems technologies for the collection, processing, storing, packaging and dissemination of information.

Internet Service Provider (ISP) – Also known as Internet Access Providers – Is a company that provides infrastructure for access to the Internet or for interconnecting other ISPs and content-based or application-based services on the Internet.

CHAPTER ONE

1.0 General Introduction

This chapter covers the basic aspects of the research. These being the introduction, statement of the problem, definition of concepts, objectives of study, rationale and justification, literature review, research questions and methodology.

1.1 Introduction

The coming of the digital age has numerous advantages. At present, most aspects of our everyday lives are easily conducted electronically through the use of computer technology and the internet. However, as our connectivity and dependency on Information Communication Technologies (ICT's) increases, so too does our vulnerability. The proliferation and integration of computer and communication technologies into every aspect of our society have inevitably led to criminal activities involving their use. Such activities, labeled with the shorthand 'computer crime' or 'cybercrime'[1], seem to be 'unique' because technology gives the ability to loot and inflict harm upon the entire world with little risk of apprehension and allows for experimenting with new varieties of criminal endeavors in the cyberspace, which is defined as an "indefinite place where individuals transact and communicate"[2] . In view of the above background, it is prudent for every nation to ensure that these advancements in technology does not make criminal activities go unaddressed. This research is therefore primarily meant to assess Zambia's legal and policy regimes in the fight against such criminal behavior perpetrated on the electronic frontier.

---

[1] The terms "cybercrime," "computer crime", "Information Technology crime," and "high-tech crime" are often used inter-changeably to refer to two major categories of offenses: in the first, the computer is the target of the offense; attacks on network confidentiality, integrity and/or availability -- i.e. unauthorized access to and illicit tampering with systems, programs or data – all fall into this category; the other category consists of traditional offenses -- such as theft, fraud, and forgery – that are committed with the assistance of or by means of computers, computer networks and related information and communications technology. This paper uses the broad definition of "cybercrime," referring to offenses falling into either category.

[2] Marjie, *Computer Forensics and Cyber Crime: An Introduction.* (New Jersey: Pearson Prentice Hall, 2004) at p.2.

1.2 Statement of the Problem

Substantive criminal law, supplemented by commercial and intellectual property protection law, may in part already prohibit a range of misconduct directed towards or involving computers or associated information technology. However, the experience of many jurisdictions is that gaps and inadequacies in traditional offence provisions necessitate the consideration of more specific laws targeting cybercrime.[3] It is in this context that the Zambian parliament passed a cybercrime specific piece of legislation entitled the Computer Crimes and Misuse Act No.13 of 2004. Under the Act, cybercrimes such as hacking, denial of service attacks and unauthorized access and modification of data have now been criminalized.

On the other hand, the use of ICT's and computer technology has greatly increased in the country. The Britannica Encyclopedia[4], records that Zambia has approximately 12,000 Internet subscribers and an additional 30,000 Internet users mainly patronising Internet cafes. Furthermore, an increasing number of people are keeping pace with technological developments by the acquisition of private home computers. Many private as well public institutions are increasingly employing computer technologies in the dispensation of their services. With this exposition, and despite the existence of the Computer Crimes and Misuse Act No. 13 of 2004, which has been on the statute book for over 4years now, there have been none if any prosecutions under the Act. This research will therefore examine some of the reasons for this position. The research also looks at the extent to which the Act covers possible criminal conduct

[3] The Zambia's Legislature acknowledged this and noted that while technological advances have brought immense benefits to society, there are also some negative developments that have come with the computer age. It was further acknowledged that the existing legal framework has often had difficulties in keeping pace with the new moral and ethical dilemmas that technology has posed. See the *Daily Parliamentary Debates For The Third Session Of The Ninth Assembly*, of Tuesday, 3rd August, 2004 from www.nationalassembly.govt.zm (Accessed: 2.06.08)

[4] http://www.britannica.com/ (Accessed: 17th July 2008)

on the electronic frontier and explores the feasibility of employing other measures in fighting cybercrime than through criminal or penal sanctions.

In addition, the fact that Government launched it's Fifth National Development Plan (FNDP)[5] and the National ICT Policy[6] after the cybercrime legislation was already in place, raises the need to assess government efforts in adressing cyber security concerns in these policy documents.[7] Similarly, the attainment of the Millennium Development Goals (MDG's)[8], generate further concerns in respect of the safety of the cyberspace and the paper examines how attainment and sustenance of the MDG's is dependent on reduced abuse of technology. Though not specifically aimed at this, the paper also considers concerns raised by the rapid expansion of e -commerce, selling and buying products and services using the Internet, which require the protection of the parties to the transactions who should be assured of a safe cyber space as well as fair dealings through the law and policy. Furthermore, with the number of internet users in the world standing at 900 million, the transnational nature of cybercrime elevates a number of problems including those of jurisdiction and international co-operation. This research would therefore also work to assess Zambia's available avenues to deal with cybercrime at regional and international levels.

1.3 Objectives of Study

The main objectives of this research are to examine whether Zambia's legal and policy regimes vis a vis cybercrime are satisfactory in ensuring safety on the electronic frontier.

---

[5] The Fifth National Development Plan was launched in 2006 and is meant to be government's main developmental governing policy until the year 2010. Hereinafter, the Fifth National Development Plan will be referred to as the 'FNDP'.

[6] Zambia's National Information and Communication Technology (ICT) Policy was launched on Wednesday, March 28th 2007 at the Mulungushi International Conference Centre in Lusaka, Zambia under the theme "ICT- For accelerated wealth and job creation" Reference to policy shall hereinafter be referred to as the 'National ICT policy'.

[7] The present Government under the leadership of President Rupiah Banda, has repeatedly emphasized its commitment in continuing the policies of the late President Mwanawasa's Government.

[8] The Millennium Development Goals were adopted at by the UN at the Millennium Summit in 2000. The Goals will hereinafter be referred to as the 'MDG'S'

The specific objectives of the study include:

1. Examine how Zambia's legal regime is measuring up with the legislative responses to cybercrime in other jurisdictions.
2. Examine whether the formal records of cybercrime in Zambia, reflects the actual level of criminal computer misconduct.
3. Identify and discuss the new and unique challenges and response issues which may be encountered during the prevention, detection and investigation of cybercrime offences.
4. Examine the feasibility of preventing and minimising the harm of cybercrime other than through criminal or penal sanctions.
5. Examine the adequacy or inadequacy of national policy measures taken by the government in the fight against cybercrime.
6. Examine how Zambia's legal regime responds to the regulation of commercial transactions conducted via the electronic frontier.
7. Examine Zambia's efforts to deal with cybercrime as a transnational crime.
8. Examine the relevant regional and international obligations and standards relating to cybercrime and assess their viability and possible concerns that they may pose for Zambia.

1.4 Rationale and Justification

The goal of the study is to examine Zambia's efforts in combating cybercrime which is increasingly becoming a global concern owing to its transnational nature. As noted earlier in the preceding sections, the world has become increasingly dependant on the use of ICT's. Zambia has been no exception to this trend. Most critical infrastructure of the country is computer technology operated. Furthermore, more services dependant on computer technology are being introduced. In Zambia, the scope for *e*-Commerce is growing largely due to increased use of electronic networks and payment systems. Examples of these include Internet Banking, ATM Machines and DDAC transactions, to mention but a few. As a matter of fact, the Government of Zambia in its' National ICT policy has affirmed to adopt an electronic governance system.[9]

[9] See Chapter 6.6 of the ICT policy (2007)

Broadly speaking will involve the deployment and exploitation of ICTs to facilitate the process of bringing Government closer to the people through major improvements in the delivery of goods and services as well as information provision in ways that are most convenient to citizens and other stakeholders. The purpose of transforming Government through ICTs is to realise efficiency gains, reduce operational and administrative costs as well as streamline government processes and procedures. The Government is aware that the potential benefits that shall be derived from the implementation of *e*-Government are enormous. In addition, the Fifth National Development Plan (FNDP) and the Millennium Development Goals (MDG's) advocate for increased use of ICT's and show how central the use of computer technology would be in the realisation of their respective objectives. These developments would however mean that people's money and confidential information as well as government infrastructure would be increasingly at stake of being electronically stolen or exposed and interfered with respectively. Furthermore, Zambia as well as its citizens are potential victims of cybercrimes which may be perpetrated from anywhere in the world. The study, would therefore operate to analyse government efforts in combating cybercrime both at national as well as at international level in light of the nature of cybercrime.

Not much literature has been generated on the subject and the author had an opportunity to examine and consider some of the works that look at the Zambian cyber laws. One such work is the research that had been conducted assessing the adequacy of the Computer Crimes and Misuse Act[10] in the fight against cybercrime.[11] The research basically focused on the Act especially the flaws therein. The research identified the inadequacies of the Act to be the lack of

[10] Act No 13 of 2004

[11] See; "The Effectiveness of the Computer Crimes and Misuse Act No. 13 of 2004 in combating cybercrime in Zambia", 2006 Obligatory Essay by Doris N. Kapumpa.

criminalization of unsolicited emails or spam as well as the want of provisio prohibiting the development and manufacture of unlawful devices for computer crime. Also identified as a shortcoming affecting the vitality the Act, the lack of enforcement mechanisms such as a special Unit of the police specialised in cybercrime.

Despite the foregoing inquiry, research had not yet been done on the assessment of Zambia's entire legal and policy regime in the fight against cybercrime. The study is significant in this respect because it will be identifying key traditional legislation which can be used to fight cybercrime as well as how the Computer Crimes and Misuse Act measures up in addressing cybercrimes with the responses taken by jurisdictions by way of a comparative law study. The diversity of this paper is also to be seen by it's examination and consideration of the advocacy of technological advancement as well as the cyber security policy issues raised in the FNDP and the newly launched National ICT policy. An examination of how these policy documents lay down guides for future reforms is also undertaken.

Furthermore, alive to the fact that criminal or penal sanctions can only be one element of the overall response to cybercrime, and that sanctions may not necessarily be the most efficient or desirable form of response, this paper, also discusses the viability of employing other ways of preventing or minimising the harm of cybercrime through means such as technological measures, regulatory controls and civil proceedings. The research is also distinct in that it examines the relevant regional and international obligations and standards relating to cybercrime and assesses not only their viability but also the possible concerns that they may pose for Zambia. This research therefore is meant to provide knowledge and also hopes to stimulate debate and further research on this important subject of cybercrime. It is also hoped that the research would also add to the working tools of the policy makers of our country.

1.6 Research Questions

1. To what extent does the Computer Crimes and Misuse Act no.13 of 2004 cover the common forms of cybercrimes?

2. To what extent do the formal records of cybercrime reflect the actual level of cybercrime incidents in the country?

3. What traditional legislation can be used to fight cybercrime and is such legislation sufficient to combat crimes on the electronic frontier in their current state?

4. What are the benefits of employing non criminal and penal modes in the fight against cybercrime?

5. To what extent does the National ICT policy (2007) consolidate cybercrime prevention and eradication efforts?

6. How much attention has the Fifth National Development Plan (2006-2010) given to the ICT sector and how would that relate to the implementation of the National ICT policy that was launched later in 2007?

7. To what extent is the attainment of the Millennium Development Goals (MDG's), dependent on a safe cyberspace?

8. Are there any regional efforts to deal with cybercrime either within the COMESA or / and SADC bodies?

9. To what extent does the Law in Zambia adequately govern commercial transactions conducted via the electronic frontier? And has Zambia done enough to deal with cybercrime as a transnational crime?

10. Are there any concerns which would come with Zambia ratifying the Council of Europe Convention on cybercrime-2001?

11. What would be merits of Zambia ratifying the Council of Europe Convention on cybercrime-2001?

1.7 Methodology

The research was done mainly by desk research. Relevant published and where necessary, unpublished works were consulted. Case law as well as other relevant pieces of legislation also made a source of information of valuable importance. An interview with Mr. Patrick Chilaizya from the Money Laundering Unit of the Anti-Corruption Commission was also conducted.

CHAPTER TWO

A COMPARATIVE LAW ANALYSIS OF RESPONSES TO CYBECRIME

2.0 Introduction

This chapter undertakes a comparative analysis of Zambia's legislative responses to the challenges of cybercrime with the approaches in other jurisdictions. The chapter also highlights the main challenges that high-tech crimes pose in this modern day and age. Owing to the increase in electronic commercial transactions, the chapter also discusses the inadequacy of Zambia's current legal system in governing such transactions.

2.1 Challenges of Cybercrime

While computer technology will be used in many traditional crimes, the nature and particular features of e-crime or cybercrime pose new and unique challenges because of characteristics such as:

(a)Anonymity[12];

(b) Transnational nature (including issues of jurisdiction, disparate criminal laws and the potential for large scale victimisation);

(c)The speed at which crimes can be committed;

(d) The volatility or transient nature of evidence, including no collateral or forensic evidence such as eyewitnesses, fingerprints, trace evidence or DNA; and

(e)The high cost of investigations.[13]

Most legal systems including Zambia's evolved and were designed to deal with real-world crime. However, with technological developments of this day, many new challenges such as those above, have emerged. Conventional crimes are now easy to commit with the aid of computer technology. For instance, it is now possible to rob or defraud someone out of his property, despite the thief and victim being in different cities or different countries. These

[12] The ability for criminals to remain anonymous on the Internet presents a huge challenge for police and policy makers. Anonymity is assisted by a proliferation of Internet cafes and web kiosks

[13] J.M. Schwarz, 'A case of identity': a gaping hole in the chain of evidence of cyber-crime Boston University Journal of Science and Technology Law 9 (2003) 90.

crimes can thus be committed with ease, at a remarkable speed and their nature makes the world borderless. Furthermore, the devastating effects of cybercrimes cannot much with those of real world crimes. For example, the *Melissa* virus of March 1999 that infected 1.2 million computers, including one in five businesses, causing $80 million in damages worldwide, caused that much damage s in only a few hours time.[14]

Most of the new forms of criminal misconduct that have emerged cannot be addressed by traditional criminal law. Thus the traditional classification of existing archaic crimes does not cater for the prosecution of most cybercrimes. A typical example is a denial of service attack[15], which cannot be prosecuted as vandalism, trespass, burglary, theft, arson, or extortion even though it is a malicious activity, damaging or perhaps even destroying the victim's ability to conduct business.[16]

The challenges of cybercrime are further compounded by the fact that traditional penal laws were not written with technology in mind, and the main problem is the applicability of this legislation on cybercrimes and to what extent. The information structure in Cyberspace represents values for governments, commerce and individuals, and should be protected also by means of the penal law. Experiences around the world have shown that a well defined rule of law that strongly deters cybercrime is critical to the effective protection of valuable information, networks and the consumers at large and it is the aim of this chapter to see how Zambia responds to the cybercrime menace.

[14] J.M. Schwarz, 'A case of identity': a gaping hole in the chain of evidence of cyber-crime Boston University Journal of Science and Technology Law 9 (2003) 92.

[15] A denial of service attack also known as a DOS attack is committed by the sending of many electronic mails to a website or server to an extent that it becomes inaccessible or very slow to utilize.

[16] See also S. W Brenner 'Cybercrime investigation and prosecution: the role of penal and procedural law' *Murdoch University Electronic Journal of Law* vol. 8(2), (2001). Available at *http://www.murdoch.edu.au/elaw/indices/issue/v8n2.html* [Accessed 25 November 2008].

2.2 A Comparative Law Analysis of Responses to Cybercrime

2.2.1 A brief background of cybercrime Legislation in Zambia

Zambia had no specific legislation meant to deal with cybercrime until the year 2004 when the legislature passed the Computer Misuse and Crimes Act.[17] The Act was passed against the background that while technological advances have brought immense benefits to society, there are also some negative developments that have come with the computer age. The legislature recognised this and it was felt that existing legal framework at the time could not keep pace with the new moral and ethical dilemmas that technology has posed and there was need for legislative intervention.[18]

The need to have specific cybercrime laws was also justified by an incident that earlier occurred in 1999 where a young Zambian hacked onto the State House website and replaced the portrait of the then serving president Fredrick Chiluba with an image of a cartoon. The perpertrator was arrested and charged with defaming the head of state contrary to S.67 of the penal code[19], but the case failed to succeed in court because there was no law in Zambia that dealt with cybercrimes.[20] The above example also goes further to give good reason for constantly keeping our law up-to-date so as to counter new forms of criminal acts that come with technological advancements.

The then Minister of Communications and Transport, Mr. Namuyamba, when introducing the Computer Misuse and Crimes Bill stressed that the intention was to meet the following objectives:

(a) to prohibit any unauthorised access, use or interference with a computer;
(b) to protect the integrity of computer systems and the confidentiality and integrity of data;
(c) to prevent abuse of computer systems;
(d) to facilitate the gathering and use of electronic evidence; and
(e) to provide for matters connected to or incidental to computer misuse and crimes.[21]

---

[17] Act No. 13 of 2004

[18] See the *Daily Parliamentary Debates For The Third Session Of The Ninth Assembly*, Tuesday, 3rd August, 2004.

[19] Cap 88 of the Laws of Zambia

[20] See Mail & Guardian Newspaper July 29 2004 from http://www.mg.co.za/ (accessed on 13th January 2009)

[21] ibid.

The National Assembly approved the Bill and was assented to by the President on the 2nd of September, 2004. The passing of the Act was a step in the right direction as it has criminalized several computer misconduct. The foregoing discussion therefore comparatively analyses how the Act responds to major criminal activities that have come forth as a result of computer technology. In achieving this, reference is made to responses taken by some individual countries as well the Council of Europe Convention on Cybercrime (2001)[22].

2.2.1 Unauthorised Access

The main criminal activity that is intended to be curbed by prohibiting unauthorized access to a computer system is hacking. Hacking has been defined as the accessing of a computer system without the express or implied permission of the owner of that computer system[23]

Unauthorised access can be gained to a system through a myriad of ways. Some hackers guess the password or do investigation in order to obtain the password to a computer, network or system. Another method is through *Back doors*[24] which are occasionally used by hackers to secure unauthorised access to computers and computer systems. There are also many software applications and devices that facilitate the unauthorised access to data.

Most countries have legislated against unauthorised access. The United Kingdom (UK), United States of America and South Africa are such examples. In the UK, unauthorized access to computer material is criminalised and causing a computer to perform any function to access a computing system without any authority is an offence.[25] The offence is committed when unauthorized access is achieved, and it is punishable on summary conviction by a fine, or six months' imprisonment, or both. In the United States, unauthorised access has been criminalized

[22] The Convention is the first international treaty on crimes committed via the Internet and other computer networks and it entered into force in July 2004. The convention is open to worldwide membership and by 1st March 2008, the convention had been ratified by 22 states and signed by another 21. Many other states are reforming their legislation using the convention as a guideline. See the *National Legislation Implementing the Convention on Cybercrime-Comparative analysis and good practice Draft paper (2008),* accessible from : Http/www.coe.int/cybercrime.

[23] D.I. Bainbridge *Introduction to Computer Law* (2000) 307.

[24] These are routes which Some System programmers sometimes leave in order to gain easy access to a computer in order to repair the computer at a later stage.

[25] See s.18 of the Computer Crimes Act (1990),

both at federal[26] and state levels and can see an offender serve for more than five years.[27] Under the Council of Europe Convention on Cybercrime, each Party is obliged to adopt such legislative and other measures as may be necessary to criminalise unauthorised access to the whole or any part of a computer system.[28] In Zambia, unauthorised access has also been criminalized. Accessing a computer system without authority or consent of the owner attracts a fine not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding two years or to both and, in the case of a subsequent offence, to a fine or to imprisonment for a term not exceeding five years or to both.[29] To completely deter activities such as hacking, it is submitted that the legislature increase the maximum sentence of unauthorized access from three years to five years and in case of a subsequent offence, the maximum sentence should be increased from the current five years to the maximum of fifteen years.

2.2.2 Unauthorised modification

The criminalization of unauthorised modification of data is to meant to help safeguard the integrity of the computer system. Data can be modified through a numerous ways. A person may for instance physically make input commands to a computer and make some modification. However, the most well known form of modification of data is through computer viruses. A computer virus is a software program that attaches or copies itself to "infect" a program and has the ability to replicate as well as infect other programs on the system. There are various other different forms of software programs that can affect computers and cause damage. Some of the most well known forms of dangerous code or programs include worms[30], Trojan horse[31] and

[26] Federal legislation governs the entire United States and is supreme and generally applicable. Individual State Laws are only applicable in a specific State.

[27] Section 1030(a) of the Federal United States Code does criminalise unauthorised access and one of the harshest sentences a hacker has ever received in the United States and was sentenced to one year's imprisonment, six months in a residential treatment program and three years probation. See G.D. Baker *Trespassers will be prosecuted: Computer Crime in the 1990s* Computer Law Journal Vol. XII No. 1 (1993) p.72

[28] Art.2 of the

[29] Computer Crimes And Misuse Act No.13 Of 2004, s.4

[30] A worm is a software program that "lives" in a computer system and prevents the system from functioning properly. It targets certain functions or resources, erases information needed by the computer and disables the proper functioning of the computer. It does not have the ability to reproduce or copy itself and therefore does not spread like a virus. A worm hides itself in the computer system.

logic bombs[32].

Legislative response world over in prohibiting unauthorised modification of computer data has been over whelming. In the US, unauthorised modification, including virus and other rogue code dissemination, could be the basis of a criminal prosecution.[33] Similarly, in the UK, unauthorized modification of computer program or data is criminalized and conviction is punishable by imprisonment not exceeding five years, or a fine, or both.[34] The Council of Europe Convention also provides that member states are to criminalise unathorised modification or interference with data.[35]

Zambia has also legislated against unauthorised modification of computer material.[36] The modification should be unauthorised and is indicative of a lack of consent. The perpetrator must know that his actions are unauthorised and should have the deliberate intent to impair the operation of the computer. It is immaterial if the modification is permanent or only temporary[37] Those convicted of this crime will be fined not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding three years, or to both. It is proposed that the maximum sentence for unauthorized modification is not sufficient and should be increased to ten years.

2.2.3 Denial of Service Attacks

The denial of service attack, also known as a DOS attack, is a common cyber misconduct that causes a computer system to be inaccessible to the intended users for a period of time.[38]There are many methods through which a denial of service can be achieved. A computer system can be bombarded with instructions or data that causes its resources to be overwhelmed and

---

[31] A Trojan horse is a useful software program that contains a secret or hidden undetectable code. When the useful software program is used the hidden code is also triggered and performs unwarranted mischievous functions.

[32] A logic bomb or a time bomb is an infection in the form of a software application designed to come into operation when a specific event takes place or at a specific preset time.

[33] In terms of section sections 1030(a)(3) and 1030(a)(5) of the Federal Code.

[34]See, Computer Misuse Act (1990) S. 3(1) & S.3 (7).

[35] Article 4 of the Council of Europe Convention on cybercrime (2001).

[36] S.6 of the Computer Crimes and Misuse Act is a key section in this regard and all forms of destructive or dangerous code will fall within the ambit of this provision.

[37] S.6(2)(b)

[38] J. Scambray *Hacking exposed* (2001) p.484

constitutes a denial of service. A common example of a DOS attack is where a cyber criminal may repeatedly sent thousands of e-mails to an e-mail address. This may cause the e-mail server to be bombarded with messages that it cannot handle and it becomes inaccessible.

Most countries do not have legislation directly curbing DOS attacks. In the United States, the Federal Code does not specifically deal with this offence though some states have specifically dealt with it.[39] The United Kingdom has no specific legislation that prohibits DOS attacks. South Africa has specifically legislated against DOS attacks. Thus section 86(5) of the Electronic Communications and Transactions Act[40] provides that:

> "A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence."

A person that is convicted of contravening this subsection may be sentenced to a fine or imprisonment not exceeding 5 years.[41]

Under the Council of Europe Convention[42], DOS attacks are covered by Art.5 which seeks to prohibit system interference. Each Party is therefore to criminalise intentional hindering, without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppression of computer data

In Zambia, DOS attacks are covered under the Computer Crimes and Misuse Act,[43] which criminalises unauthorized obstruction of use of computer.[44] This would encompass situations such as where one interferes with, interrupts, or obstructs the lawful use of a computer; or causes direct or indirectly, a degradation, failure, or other impairment of function of a computerized system or any part thereof. This provision is very instrumental against acts such as denial of service attacks, where criminals would send a lot of emails to a website or computer

[39] North Carolina is such an example, see Section 14-456 of the General Statutes of North Carolina
[40] Act 25 of 2002
[41] Ibid, Section 89(2)
[42] Council of Europe Convention on Cybercrime (2001)
[43] Act no. 13 of 2004
[44] ibid, s.8

system so as to make it unable to operate efficiently. Under the Act, a person who without authority obstructs the use of a computer or a computerized system or any part thereof is liable on conviction to a fine not exceeding five hundred thousand penalty units or to imprisonment for a term not exceeding ten years, or to both.[45]

2.2.4 Unsolicited electronic mail (Spam)

The internet makes it possible to use forms of advertising that has raised concerns world over. It is now a common trend for advertisements to come in form of unsolicited electronic mail (Spam) sent to ones email addresses. The problem with such form of advertisements is that it not only impinges on the privacy of individual Internet users but also creates economic losses and as well as time-related losses in terms of the time spent reading and deleting the messages[46]. It is currently estimated that 60 per cent of all email messages are spam.[47] The situation is compounded further because some unsolicited mails are meant to swindle innocent internet users of their money, etc.

Most jurisdictions have legislated specifically to address spam. In South Africa for example, a merchant who sends unsolicited electronic communication ("spam") must provide the consumer with the option to cancel its subscription to the mailing list, and must identify the source from which that merchant obtained such consumer's personal information. No agreement may be concluded if the consumer has not responded to the spam. Failure to comply with this provision attracts a fine or imprisonment for a period not exceeding twelve months.[48] Furthermore, it is an offence under the South African laws to send an unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome and if found guilty one can serve no more than 12 months.[49] In the United States, a new federal bill called the

[45] ibid
[46] European Commission Report, (2003) p.34
[47] E. Moustakas, C. Ranganathan & P. Duquenoy, *Combating Spam Through Legislation: A Comparative Analysis of US And European Approaches* (2006) p.19
[48] See Sections 45(1),(2) & (3) of the Electronic Communications Transactions Act No.25 of 2002
[49] S.45(4) of the Electronic Communications Transactions Act No.25 of 2002 as read together with s.89(1)

Controlling the Assault of Non-solicited Pornography and Marketing (CAN-SPAM) Act was signed into law in December 2003. The Act represents a 'compromise' between the various spam stakeholders and allows e-mail marketers to send unsolicited commercial emails until the consumer optsout from receiving future messages. [50] It also requires e-mail marketers to identify UCE as advertisements, as well as to include warning labels on UCE that contains sexual material.[51] It is also a requirement under the Act also requires that commercial e-mail should include the sender's valid physical address and recipients must be given an opt-out method. Convicted spammers could face penalties of up to five years in prison.[52] The Council of Europe Convention also advocates for the criminalization of spam.[53]

In Zambia, spam has not been fully legislated against. The Computer Crimes and Misuse Act[54] does not specifically criminalise or prohibit the sending of unsolicited electronic mail or spam. Spam would only be illegal if it causes damage or impairs the operation of a computer.[55] This unfortunately encourages the invasion of people's mail boxes and is an area that needs legislative intervention. Zambia may draw from approaches taken by South Africa and the United States in dealing with spam.

2.2.5 Unauthorized Interception

Unauthorized Interception is meant to criminalise the interception and monitoring communications sent via the Internet or other information networks. Most criminals seek to further their criminal activities through means such as intercepting data by tapping the communication line between two computers through the use of equipment or monitoring data that are sent via a network. Criminalizing such conduct, is a essential to ensure confidentiality and safety.

---

[50] E. Moustakas, C. Ranganathan & P. Duquenoy, *Combating Spam Through Legislation: A Comparative Analysis of US And European Approaches* (2006) p.5

[51] Can Spam Act of 2003, s.5

[52] ibid, s. 877

[53] Art. 5

[54] Act no. 13 of 2004.

[55] See S.8 of the Computer Crimes and Misuse Act No. 13 of 2004. By way of extension, Section 12 would also come into play if spam causes a computer to cease to function.

Several countries have legislated against unauthorised interception. The Electronic Communications Privacy Act[56] of the United States, criminalises the unauthorised interception of an electronic communication. The interception of an electronic mail message being sent across a network will constitute an offence.[57] The UK has no such specific legislation. South Africa is another country that has legislated against unauthorised interception and the penalty is a fine or a term of imprisonment not exceeding 12 months [58] Unathorised interception of data communications by electronic means is also to be criminalized by member states of the Council of Europe Convention[59]. In Zambia, unauthorized interception is prohibited under s.7 of the Act[60] and if convicted, one is liable to a fine not exceeding two thousand penalty units or to imprisonment for a term not exceeding five years, or to both. This is fair legislative response.

2.1.6 Pornography

Pornography is one aspect that has been on the rise with the coming of the digital age. Pornographic materials are widely distributed through the Internet[61] and a concern is that Information networks and computers are instrumental in the creation, possession and distribution of pornography.

In most jurisdictions, the concern is child pornography and little apprehension is expressed for pornography where adults are involved. In the UK, the Protection of Children Act[62] regulates child pornography by criminalising taking, permitting to be taken or making, distributing or showing, possessing, publishing or causing to be published any indecent photograph or indecent pseudo-photograph of a child, including by electronic and other means capable of converting

---

[56] (1986)

[57] See C.W. Darryl 'Viewing Computer Crime: Where does the systems error really exist?' Computer Law Journal Vol. XI (1991) p.272 .

[58] See, The Electronic Communications and Transactions(ECT) Act No.25 of 2002, s.86(1) & s.89(1). Note that the sentence under the South African ECT Act is lighter compared to that imposed in Zambia. Our legislature in Zambia have attached the necessary gravity to unauthorised interceptions which may cause unprecedented losses.

[59] See Art.3

[60] The Computer Crimes and Misuse Act No. 13 of 2004

[61] M.Hirst *Cyberobscenity and the Ambit of English Criminal Law* Computers & Law Vol. 13 (2002) Issue 2 p.25.

[62] (1978)

into a photograph.[63] The punishment for this offence is imprisonment for a period not exceeding ten years, or a fine, or both.[64] The United States and South Africa are other countries that legislated against child pornography perpetrated *inter alia* via the electronic frontier.[65] The Council of Europe Convention also criminalizes child pornography.[66]

In Zambia, child pornography is penalized under s. 177A of the Penal Code Act[67]. Under subsection 2(b) of the section,

> Any person who sells to a child pornographic material or compels a child to watch a pornographic film or view pornography on the internet or elsewhere or in any form intended to corrupt a child's morals; commits an offence and is liable, upon conviction, to a term of imprisonment of not less than fifteen years.[68]

The law thus adequately covers child pornography on the electronic frontier. However, S.177 of the Penal Code Act[69], which seeks to cover pornography generally, is couched in a way that presupposes the conventional possession or access of pornographic materials.[70] It is therefore doubtful whether accessing or browsing of pornographic sites would be said to be covered by S.177 without downloading the content to the computer hard disk. There is need in this regard to specifically prohibit access to internet sites.[71]

---

[63] See the Protection of Children Act of 1978 (c. 37) s 1 as amended by the Criminal Justice and Public Order Act of 1994 (c. 33) and the Sexual Offences Act of 2003 (42). Available at *http://www.geocities.com.pca_1978/reference/pca_1978amSOA.html* [Accessed November 3, 2008].

[64] See the Protection of Children Act s. 6.

[65] See for example S.27(1)(a) of the Films and Publications Act 65 of 1996 of South Africa

[66] See Art. 9 of the Council of Europe Convention on Cybercrime 2001. The Convention uses the term "minor" to refer to children under the age of eighteen. This is in accordance with the definition of child under the United Nations Convention on the Rights of the Child. However, the drafters recognized that some countries have a lower age for "minors" and allow Convention parties to set a different age-limit, provided it is not less than 16 years of age.

[67] Cap 87 of the laws of Zambia, as amended by Act No. 15 of 2005

[68] A child for the purposes of the section is a person below 18 years of age. This is similar to the age limit in most jurisdictions. The UK and South Africa are such examples.

[69] ibid

[70] For example, s177A 2(b) is more clearer in catering for internet pornography than section 177. (1)(a) which provides that a person is guilty if that person 'makes, produces or has in his possession any one or more obscene writings, drawings, prints, paintings, printed matter, pictures, posters, emblems, photographs, cinematograph films or any other object tending to corrupt morals'

[71] See, Doris N. Kapumpa, "The Effectiveness of the Computer Crimes and Misuse Act No. 13 of 2004 in combating cybercrime in Zambia", 2006 Obligatory Essay

2.2.7 Manufacture of Devices furthering cybercrimes

Most jurisdictions have prohibited the manufacture of devices or software that is meant to further cybercrime. In the UK the making, supplying or obtaining articles for use in computer misuse offences is criminal. Thus the developing, owning and distributing 'hacker tools' for criminal use is curbed[72] This also covers distributing these tools believing that they are 'likely to be used' criminally[73] Council of Europe Convention, obliges its member states to criminalise the production, sale, procurement for use, import, distribution or otherwise making available devices e.g. computer viruses, or other malicious programs designed for commission of cybercrime. In Zambia, the legal regime does not criminalise the manufacture of devices meant to further cybercrimes. This area needs legislative intervention so that criminal activities in the cyberspace are not indirectly promoted through such *lacunae*.

2.2.8 Computer-Related Fraud

Traditional fraud is committed where one unlawful and intentionally makes a misrepresentation which causes actual prejudice or which is potentially prejudicial to another. Computer related fraud involves the unauthorised commanding or alteration of a computer system or data which results in loss of property for an economic benefit for oneself or for another person. Fraud can be perpetrated through the Internet and electronic mail and these types of actions are commonly referred to as online fraud.

The current trend world over is that countries are now criminalizing computer related fraud. In the United States there are various statutes that criminalize some form of online fraudulent conduct. For example, Section 1030(a)(4) of the United States Criminal Code prohibits unauthorised access to a protected computer with the intent to defraud and obtaining something

[72] See the Police and Justice Act s 37
[73] ibid, s 37(2).

of value. In South Africa, the Electronic Communications Transactions Act[74] has specifically criminalised computer related fraud[75]

Similarly, the Council of Europe Convention on Cybercrime under Article 8 of makes computer-related fraud illegal and member states are to legislate accordingly. In Zambia, computer-related fraud has not specifically been legislated against and the Penal Code Act [76] which is meant to counter traditional fraud has remained un-updated despite the eminent need to have legislation that is technologically accommodative.

2.2.9 Computer-Related Forgery

Most criminal law systems criminalise the forgery of tangible documents. However, forgery of electronic data or documents is one area that has not been legislated against in many jurisdictions. South Africa is one of the few countries that has specifically criminalised computer related forgery. The production of fake data with the intent that it be considered or acted upon as if it were authentic, is an offence under South African laws.[77] Under the Council of Europe Convention, computer related forgery has been criminalised and Art.7 creates a parallel offence to the forgery of tangible documents. The Article aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data.

Zambia has not updated its laws to deal with computer related forgery. The Penal Code[78] still provides for forgery in terms of tangible documents.[79] This area requires legislative intervention in view of the technological advancements that have been made.

---

[74] Act No.25 of 2002
[75] Under s.87(2)
[76] Cap 87 of the Law of Zambia
[77] See s.86(2) of the Electronic Communications Transactions Act No.25 of 2002
[78] Penal Code Act Cap 87 of the laws of Zambia
[79] Ibid, see s. 344

2.2.9.1 Infringement of Intellectual Property Rights

Infringement of intellectual property rights using computer technology is a problem that is now on the increase. Unauthorized copying, selling, distribution and distortion of copyright protected products is made easy with the use of the computers as well as the internet. In the UK infringement of Intellectual Property rights is criminalized in the Copyright, Designs and Patents Act[80] . This law criminalises copyright infringement for unlawfully making for selling or hiring, selling, hiring, importing, possessing, offering for selling or hiring, publicly exhibiting, distributing or copying copyright.[81] Under this law copyright also extends to computer programmes.[82] Conviction is punishable by imprisonment for not more than two years, or a fine, or both.[83]

The Council of Europe Convention has also criminalized offenses related to the Infringements of Copyright and Related Rights. Thus under the Convention, member states are to legislate against those offences that "are among the most commonly committed offences on the Internet, i.e. the reproduction and dissemination on the Internet of protected works, without the approval of the copyright holder. The Copyright offences "must be committed 'willfully' for criminal liability to apply."[84] "Willfully" was substituted for "intentionally," because this term is employed in the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"), which governs the obligations to criminalize copyright violations.[85]

In Zambia, the relevant legislation with regard to infringement of intellectual property rights is the Copyright and Performers Rights Act[86]. The Act criminalizes infringement of copyright and related rights. The Act prohibits unauthorized copying, reproducing and disseminating of

---

[80] (1988)
[81] Copyright, Designs and Patents Act of 1988 (c. 48) s 107
[82] Ibid, s 3(b).
[83] Ibid, s 107(4).
[84] Art.10
[85] M. Keyser, *The Council Of Europe Convention On Cybercrime* , Journal of Transnational Law & Policy (2003) Vol. 12(2) p. 309
[86] Cap 406 of the Laws of Zambia

copyright protected works.[87] Although Zambia's copyright law does not explicitly address offences committed by via the electronic frontier, copyright infringement perpetrated through the internet or other electronic may still be captured.[88]

2.2.9.1 Theft

Theft on the electronic frontier, raises two major challenges that conventional criminal law cannot adequately address. Firstly is the definition or interpretation of what constitutes property for purposes of committing the offence of theft. Theft as an offence, stems from the common law position that only tangible things can be stolen.[89] This is problematic in view of the fact that computer technology now makes it possible and easy to steal intangibles such as data or information. The other main challenge is the new phenomenon of identity theft. Identity theft describes criminal acts where the perpetrator fraudulently obtains and uses another person's identity using internet technology.[90]

Few jurisdictions have legislated to specifically address the two challenges of theft of information and identity theft. Under the UK laws, the issue of theft of information is not addressed and neither does the Computer Misuse Act[91]. The definition of property in the Theft Act[92] does not include intangible information. In the case of **Oxford v Moss**[93] a student copied an examination paper and was prosecuted of theft of information in terms of the provisions of the Theft Act and it was contended that the paper was an article of value.[94] The student was

[87] See s.17, of the Act which lists controlled acts in relation to copyright protected works. This provision is further reinforced by s. 18 which provides that copyright is infringed by doing controlled acts in relation to the protected work.

[88] For a detailed discussion of Zambia's Intellectual Property law, see G. Kanja *Intellectual Property Law,* (UNZA Press : 2006).

[89] For instance in the English case of **R v Absalon [1979] 68 Cr App R 183** it was held that data of an oil company, although very valuable, did not constitute property for purposes of theft.

[90] It must be noted however that although these acts can be carried out without the help of technical means, theft of identity on the internet is not only a new phenomenon but is one that is on the increase and therefore justifies legislative response.

[91] (1990)

[92] Theft Act 1978 (as amended by the Theft Amendment Act (1996)

[93] 1968.

[94] [1978] 68 Cr App R 183.

acquitted of theft of information under the Theft Act on the basis that information is not included in the definition of property.[95] Similarly, Canada is still behind and the case of **R v Offley**[96] avows that information cannot be the subject of theft. In the US, certain states have clearly included incorporeal property is to be capable of being a subject of theft.[97]

In Zambia, theft of information or intangibles property may not necessarily be a subject of theft. This is because the law does not specifically prohibit theft of intangibles and is couched in the sense that theft should involve the physical taking and moving of someone else's property.[98] For instance, under the Penal Code Act[99] a person shall not be deemed to take a thing unless he moves the thing or causes it to move.[100] Such provisions much discretion to the courts to decide whether intangible property can be a subject of theft. This area requires legislative response so that property may be specifically defined to include intangible things such as data, and information.

Identity theft as noted above, is yet another challenge that conventional criminal law fails to combat. In the UK the Identity Cards Act 2006 contains a number of offences concerning the possession of false 'identity documents'[101] and providing false information.[102] However, other than the provisions under the Identity Cards Act 2006, no such offence has yet been established.[103] South Africa has not also specifically legislated against the identity theft and identity theft provisions are absent in the Council of Europe Convention on cybercrime 2001. The United States has the Identity Theft and Assumption Deterrence Act of 1998, which establishes a range of offences related to the abuse of identification documents, including:

---

[95] Edwards, Savage & Walden (editors) Information Technology & The Law (1990) 150.
[96] (1986) 28 C. C. C. (3d) 1.
[97] The Delaware Code for instance contains defines 'property' as anything of value including data. See Section 931 (11) of the Delaware Code.
[98] See s.264 of the Penal code Act Cap 87 of the Laws of Zambia.
[99] Cap 87 of the Laws of Zambia
[100] s.265 (5) of the Penal code Act Cap 87 of the Laws of Zambia.
[101] Identity Cards Act 2006, s 26(1).
[102] ibid, ss 25 and 28 respectively.

Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, any unlawful activity[104]. The tariffs under the Act range from five years' to fifteen years' imprisonment.[105] In 2004, the Act was amended to insert an offence of 'aggravated identity theft',[106] which imposes additional prison terms on those who knowingly transfer, possess or use a means of identifying another person in the course of the commission of a felony or terrorist offence.[107]

In Zambia, no legal provisions exist to specifically tackle identity theft. A perpetrator can however be prosecuted for various other offences that may ensure from the use of another persons' identity. Nevertheless, having a specific provision prohibiting identity theft would be very useful and reduce chances of offenders going free due to loop holes in our laws. This would also have a deterrent effect on would-be offenders.

2.2.9.2 Inter-jurisdictional and Procedural aspects.

Other issues to note about Zambia's legal regime on combating cybercrime include the jurisdictional and procedural aspects. The Computer Crimes and Misuse Act has fairly covered these important issues. It must also be mentioned here that with respect to jurisdictional aspects, a states has inherent jurisdiction to try offenders who commit crimes within their national geographical territory.[108] It would therefore follow that special circumstances would have to be present for a country to claim jurisdiction to try offences which have been committed outside its territorial borders.[109] In this connection, the Act does recognize this limitation of the national courts' jurisdiction and provides that a cybercrime committed abroad shall fall within the

---

[104] 18 USC § 1028(a)(7).
[105] 18 USC § 1028(b).
[106] Identity Theft Penalty Enhancement Act of 2004, HR, 1731
[107] Codified at 18 USC § 1028A.
[108] This is an act of state sovereignity.
[109] For a detailed discussion of the types of jurisdictions which a country would claim in certain circumstances, see: Harris, D.J. *"Cases and Materials on International Law"*, Sweet & Maxwell London 2003, Thirteenth edition

jurisdiction of our courts and thus be treated as if they were committed within, if any of the following conditions exists:

(a) the accused was in Zambia at the material time;
(b) the computer, program or data was in Zambia at the material time; or
(c) the damage occurred within Zambia whether or not paragraph (a) or (b) applies.[110]

The idea is that for one to be prosecuted for an offence in any jurisdiction, there has to be a material link between the offender and the prosecuting state or that the effects were felt on the prosecuting state. This approach is in conformity with international standards.[111]

For procedural aspects, the Act has given search and seizure powers to the police and has allowed for admission of electronic evidence.[112] Through such provisions, the Act further enhances computer security as it broadens the powers of the police to investigate such misdeeds.

2.3 E-commerce and the inadequacy of traditional legislation

E-Commerce is one of the most exciting and far-reaching uses of the Internet and new ICT technology. Consumers now have a world of products available to them and businesses have new opportunities to reach customers, sell products, and develop niche markets. The existing legal structure in Zambia was developed in a paper-based economy. The law gives special treatment to documents and documented evidence. In a new e-economy, standards, rules and legislation must be established that provide the same protective infrastructure that exists for paper-based transactions. Thus, one of the most important areas to deal with is the development of legislation that creates an enabling and nurturing environment for e-Commerce by making legal requirements for transactions "media neutral."[113]

---

[110] S.3(2)
[111] See C.W. Darryl 'Viewing Computer Crime: Where does the systems error really exist?' Computer Law Journal Vol. XI (1991) p.298.
[112] See S.16 of the Computer Crimes and Misuse Act no. 13 of 2004.
[113] It has also been acknowledged in the National ICT policy 2007 that Zambia has inadequate laws and legal system to support E-Commerce. See Chapter 2.7 of the policy.

There is no e-Commerce legislation dealing with contracts.[114] Zambia also has limited legislation dealing with electronic records.[115] The government has affirmed in the ICT policy (2007), that it would develop effective laws and regulations that shall govern E-Commerce at national level supported by regional and international systems.[116] Many countries world over have legislated in the area of electronic commercial transactions. South Africa for example passed the Electronic Communications Transactions Act[117] which deals *inter alia* with electronic transactions. The Act has addressed a number of pertinent issues. For example, no information is to be deemed not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message[118]. A requirement in law that a document or information must be in writing is met if the document or information is still met even if it is in the form of a data message provided it is accessible in a manner usable for subsequent reference.[119] Similarly, an electronic signature under South African laws is not without legal force and effect merely on the grounds that it is in electronic form.[120]

The technological advancements, growing increase in electronic commercial transactions and the intended e-government system that government seeks to promote[121], justify the need for Zambia to adopt an appropriate legal framework to govern and regulate electronic transactions.

---

[114] A contract is formed as soon as there is consensus between the parties to the contract i.e. as soon as the offeree has legally accepted the offer. Where the parties are not in each other's presence, questions as to when and where the contract has been concluded, have resulted in many legal uncertainties. However, most jurisdictions (South Africa, Australia and UK) have taken the old common law approach that where an instantaneous method of acceptance of an offer is used, eg telex or email, then the contract is made when and where it is received. See the cases of **Entores v Miles Far East Corp [1955] 2 QB 327** and **Brinkibon v Stahag Stahl [1983] 2 AC 34.**

[115] . This includes the Computer Crimes and Misuse Act No. 13 of 2004 which provides for admission of electronic evidence, see S.16 (4) (iv).

[116] This would most likely be based on the UNCITRAL Model Law on Electronic Commerce. This Model Law has provided the essential base for legislation throughout the world and would allow Zambia to establish a consistent approach to e-Commerce equivalency. UNCITRAL also developed a *Model Law on Electronic Signatures* to help avoid the risk that different countries would develop divergent approaches to electronic signatures

[117] Act No.25 of 2002 based on the UNCITRAL Model Law on Electronic Commerce.

[118] Electronic Communications Transactions Act No.25 of 2002, S.11. (1)

[119] Ibid, S.12

[120] Ibid, S.13

[121] The National ICT policy (2007) does show governments commitment towards promoting e- governance and e-commerce in Zambia.

2.4 Conclusion

This chapter has examined and considered the challenges of cybercrime. Furthermore, the comparative law analysis with several jurisdictions has revealed that the Zambia still lacks behind in combating cybercrime owing to non criminalisation of certain serious cybercrimes. Notable of these are identity theft, manufacture of devices for purposes of furthering the commission of cybercrimes and the sending of unsolicited electronic mail. The present three years maximum sentences for the offences of unauthorized access and unauthorized modification does not send a good message to would-be offenders and thus require revisiting by the legislature. In addition, Zambia's legal regime, has not taken into account the fact that if traditional legislation is to tackle technologically perpertrated conventional crime, there is need to amend the law so that it suits such developments. This is evident for the offences of computer related forgery, computer related fraud, theft, pornography and intellectual property rights infringement.

E-commerce is one area that has been identified as requiring an appropriate legal framework that would govern electronic commercial transactions and clearly lay down the rules and regulations of contract law that should be taken in an electronic setting. Zambia may draw from approaches taken by South Africa.

CHAPTER THREE

AN ASSESSMENT OF ZAMBIA'S POLICY MEASURES VIS A VIS CYBERCRIME

3.0 Introduction

This chapter looks at the Zambia's policy measures in the fight and prevention of computer technology abuse. Particular attention is paid to the newly launched National ICT policy[122] as well as the Fifth National Development Plan (FNDP)[123]. The FNDP which is the nations' major policy guide, is looked at *inter alia* in terms of governments' commitment towards developing the ICT sector with particular attention on the security measures. Also discussed under this chapter is the role of ICT's in the attainment of the Millennium Development Goals (MDG's)[124] as well as the increasing need to ensure a reduced abuse of computer technology in the process. Goal number 8 of the MDG's is given particular attention in view of its advocacy of ICT development. Lastly, the chapter concludes by discussing the feasibility of employing non penal or criminal sanctions in the overall response to cybercrime.

3.1 The National ICT Policy (2007)

In view of the huge benefits that come with ICT's, legislative and public policy measures may encourage communities, organisations and individuals to invest in and use Information and Communication Technologies (ICTs). However, to have a better public policy and legal framework on ICT, it is necessary that utmost attention is paid to ensuring that criminal activities such as cybercrime which would flourish with the wide use of ICT are curtailed. The foregoing therefore justifies the urgency of analyzing how the National ICT policy addresses concerns regarding deterrence of using ICT's to further criminal activities involving computer technology as well as how the policy lays down guides for future legislative reform.

[122] The ICT policy was launched in 2007.
[123] Herein after referred to as the FNDP.
[124] Herein after referred to as the MDG's

The Zambian government prepared the National ICT Policy of 2007 to coordinate all matters related to ICT in the country.[125] The goals of the ICT policy are grouped into thirteen main areas. These are:

i. Promoting Human Resources Development
ii. Promoting ICT in Education, Research & Development
iii. Promoting Public Access, Content Development and Cultural Heritage
iv. Developing the ICT Sector
v. Developing Telecommunications & Supporting Infrastructure
vi. Promoting Electronic Government
vii. Promoting Electronic Commerce
viii. Promoting the Integration of ICT in Agriculture Development
ix. Promoting the Integration of ICT in Healthcare Delivery
x. Promoting the Integration Of ICT in Tourism, Environment & Natural Resources Management
xi. Mainstreaming Youth And Women Issues
xii. Developing the Legal & Regulatory Framework
xiii. Promoting Security in the Information Society

Most of the above listed goals aim at furthering the use of ICT in the country. However, as alluded to earlier in the preceding chapters, ICT's also offers opportunities to criminals to commit undesirable acts with ease and little risk of apprehension. It is in this vein that the necessity of evaluating government's commitment in the ICT policy vis a vis tackling such activities is founded. Thus of much concern to the theme of this paper are the last two policy goals under the National ICT policy i.e. 'Developing the Legal & Regulatory framework' and 'Promoting Security in the Information Society'. A detailed analysis of these two policy goals is what the succeeding units embark upon.

[125] The ICT sector in Zambia is categorized into four main sub-sectors, namely; Telecommunications, information technology, electronic media and postal communication system. However, special attention is accorded to the information technology sub-sector as it directly falls within the realm of this research. At present the ICT sector is mainly regulated by the Communications Authority of Zambia (CAZ) and the Ministry of Communications and Transport. The CAZ is responsible for regulating the provision of internet and telecommunications products and services in the country. Its specific functions include issuing licenses and promoting the interests of consumers and other users of ICT services/ products as well as ensuring that the benefits of the sector accrue to the nation at large. On the other hand, Ministry of Communications and Transport regulates the postal sub-sector and broadcasting services.

3.1.2 Developing the Legal & Regulatory framework: *Policy goal number 12*

The National ICT policy acknowledges that an appropriate and dynamic legal/regulatory framework is mandatory to act as the foundation for the development of the ICT sector. It is further highlighted that the current legal and regulatory framework is inadequate in addressing the current market challenges.[126] Therefore it is the goal of the policy to develop appropriate institutional, legal and regulatory system in order to support the development of a competitive local ICT sector based on convergence principles; supported by fair, predictable, and transparent legal and regulatory framework.[127]

In order to achieve the above goal, the government has made a number of commitments and only the main ones will be looked at. To start with, the government aims at putting in place relevant and effective laws and regulations aimed at adherence to national, regional and international standards and best practices. Having the relevant and effective laws that are in conformity with regional and international standards and best practices is important in the cybercrime arena in view of the transnational nature of the crime. Furthermore, being part of regional and international efforts on a particular subject also fosters co-operation among nations. Also espoused in the ICT policy is government's intention to promote professionalism in ICT industry. The benefits of this are numerous and the most notable one is that professionalism would mean having well trained human resources that would be able to make meaningful contributions in making the cyberspace safer. For instance, professionalism would provide a better foresight of different threats in the ICT sector such as those that affect the integrity of systems. At present, the only body that seeks to set standards for IT personnel in the country is the Computer Society of Zambia which unfortunately, does not have power to regulate the training of all IT professionals, register or discipline them.

Another important aspect that may highlighted as being important in the goal of developing an appropriate legal and regulatory framework for the ICT is that of creating specific laws to

[126] See Chapter 6.12 of the ICT policy.
[127] Ibid,

support E-Services.[128] This is a very important measure that requires much urgency in view of the increasing use of E-services and the inadequate conventional legal regime that is tailored for paper transactions.

Also remarkable of the aims of government vis a via improving the ICT sector is the establishment of an ICT tribunal.[129] The tribunal would be designed to address only appeal cases arising from rulings or directives of the Regulator[130] as the first line of dispute resolution among parties in the sector. The advantages of having appeal tribunals are numerous. Tribunals tend to reduce on the cases that ultimately reach our already crowded formal court system. Other strengths of tribunals are in the expeditious handing of cases and the few formalities involved. Despite the many virtues that may arise in having an appeal tribunal, there is a major challenge for the government of clearly defining the role and powers of the intended ICT Tribunal.

3.1.3 Promoting Security in the Information Society: *Policy goal number 13*

This goal stems from the realization that Zambia like most countries in the world is vulnerable to some of the negative implications that may hinder the mainstreaming of ICTs in society. [131] Therefore it is the aim of the policy to safeguard national, institutional and individual security concerns to support the development, deployment and effective use of ICTs.

In order to attain the policy goal of promoting security in the information society, the government intends to embark on several measures. Firstly, it is governments' aim to establish a Computer Crimes Investigation Unit for cyber law enforcement and the National Electronic communication Security Centre.[132] These bodies would fall within the internal organs of specialised security agencies. This is would be advantageous in that establishing independent units may not only be very costly, but would also require a long time.

---

[128] See Policy goal number seven
[129] Chapter 6.12.2(e)
[130] The regulator in this case may include the CAZ and the Ministry of Transport and Communication.
[131] See Chapter 6.14 of the ICT Policy
[132] Chapter 6.13.2(a)

The intention to establish a Computer Crimes Investigation Unit is a welcome move and should be encouraged at all costs in view of the presently lacking expertise in the enforcement of cyber laws. The Unit would thus play a remarkable role in preventing, detecting and responding to cybercrime and misuse of ICT and contribute to the fight against national, regional and international crimes such as pornography, fraud, money laundering, drug trafficking and terrorism. The National Electronic Communication Security Centre is another instrumental body that would complement the efforts of safeguarding information and communication infrastructure, networks and systems. It is indeed true that the two bodies as highlighted in the policy[133], would help as part of the reform process to: ensure the availability, authenticity, integrity and confidentiality of Government, public and private communication networks and systems; data and information content integrity; consumer privacy and protection as well as address security issues aimed at damaging or corrupting Zambia's cultural heritage, national image and identity.

Understanding that the ICT security bodies need be given the necessary equipment, the government has thus aimed at deploying ICTs to facilitate, support and enhance the management, operation and administration of security matters as well as the command and control structure of National Security Agencies. The security personnel also have to be trained and this has been acknowledged by the government by its commitment towards implementing ICT skills development within the Security Agencies to support effective deployment and application of ICTs in operations and service delivery.[134] The security of the ICT sector would further be enhanced with coordinated among security agencies. Gladly, there seem to be commitment in the National ICT policy[135] towards ensuring cross-sectoral linkages and co-ordination among security agencies a move that would remarkably help in the bid to adequately address ICT related security concerns.

[133] Ibid,
[134] See chapter 6.13.4 (d) and (e) of the ICT policy
[135] Chapter 6.13.3(d)

The government also intends to enact and enforce legislation that allows for effective investigation and prosecution of cyber related crimes.[136] However in view of the fact that criminal law would not fully protect society from high tech crimes, the government has acknowledged the need to outrun that and compel all organizations providing public information services such as telecommunication services, Internet, email to deliberately incorporate administrative, technological and other such practical measures to enable national security agencies to curb cybercrime.[137] This is another virtue in the policy because the employment of administrative and technological measures would operate as preventive measures in the fighting cybercrime. This is further supported by the immerse effects that may be caused by cybercrime. For example in May 2000 a virus that originated in the Philippines and spread rapidly throughout the world, destroyed files and stole passwords. The virus affected NASA and the CIA on its two-hour race around the world. The virus is estimated to have ultimately affected over forty-five million users in more than twenty countries. The various estimates of the damage caused, ranging from two billion dollars up to ten billion.[138] The foregoing exposition therefore reflects on the inherent difficulty of assessing the harm that may be inflicted by cybercrime and goes to show that the preventive approach is better than a reactive one. The use of administrative, technological and other such practical measures in preventing cybercrime should therefore be supported fully.

Another measure to be undertaken by the government is the implementation of ICT Security awareness programmes amongst corporate and users as well as the general public.[139] This would have a great impact on the safety of the cyber space because people would be made aware of cyber laws as well as the extent of their freedom to use computer technology. The awareness programmes would also contribute a great deal to enhance user confidence and trust among the public.

---

[136] Chapter 6.13.2(c)
[137] Ibid, subsection (b)
[138] See M. D. Goodman and S. W. Brenner ' The Emerging Consensus On Criminal Conduct In Cyberspace' (2003) p.5
[139] Chapter 6.13.4(b)

In sum, the ICT policy sets out a number of valuable measure towards ensuring that the much advocated use of ICT does not provide a fertile breeding ground for cybercrime. The intention to establish a Computer Crimes Investigation Unit for cyber law enforcement and the National Electronic communication Security Centre is a welcome move in ensuring cyber safety. The challenge however would be the definition of clear roles and responsibilities among these bodies and other key players including policy makers, regulators and operators. Furthermore, the establishment of the ICT Tribunal designed to address cases arising from rulings or directives of the *Regulator* as the first line of dispute resolution among parties in the ICT sector is yet another virtue that may be identified in the policy.

The public cyber security awareness programmes as well as the provision of the necessary ICT's to the various security agencies should also be commended as being a good objective. The advocacy of administrative, technological and other practical measure in cyber security is yet another virtue worth a commendation. However, despite having good intentions there is need for genuine commitment action towards that attainment of the policy's goals. The government should therefore provide political and economic will, vision and leadership to facilitate and drive the development of the ICT sector.

3.2 The Fifth National Development Plan (2006-2010) and the ICT sector

The Fifth National Development Plan is a policy document highlighting the areas of focus which the government intends to embark upon in the period 2006 to 2010.[140] The FNDP was launched in 2006 a year before the National ICT policy was finalized. This section basically tries to see *inter alia*, how much attention or priority the FNDP accords to the ICT sector. This is further justified in view of ascertaining whether the attainment of the policy measures in the ICT policy discussed in the preceding section would require radical changes in Development Plan vis a vis the ICT sector.

[140] The FNDP like the ICT policy, was also launched by the Levy Mwanawasa led administration, however, the succeeding government has expressed commitment towards ensuring continuity with the policies of the Mwanawasa regime. See the MMD manifesto, 2008 presidential elections at p.23

ICT is one of the fastest growing industries in the world and is changing technologies, business models, and work relations. It is widely and increasingly regarded as the fourth factor of production after land, labour, and capital. The Government is alive to this fact and focuses at three levels namely, Connectivity, Capacity and Content.[141]

The government had set areas of focus in the ICT sector not so different from those in the 2007 National ICT policy. In respect of the policy, legal, and institutional reforms, it is the aim of the FNDP to develop and monitor the implementation of appropriate policies, legal, and institutional frameworks to foster the development of sustainable information and communications sub-sector.[142] Furthermore, to ensure a safe and friendly information and communication technology system the Government prioritized the areas of education and enforcement. The National ICT policy is in consonance with the foregoing as it also advocates for awareness programmes for ICT security and the institution of effective law enforcement mechanisms such as the creation of cybercrime investigation unit.[143] The FNDP also highlights the need to develop and implement bilateral and multilateral agreements in the ICT sector as well as ratify and domesticate conventions, protocols, and agreements to guarantee safe usage and enable the maximum benefits of computer technology accrue to the Nation.[144]

In light of the foregoing, it is evident that Government has remained consistent with improving the security in ICT sector and ensuring that criminal activities in the sector do not go unpunished. This is so because of the unswerving affirmation of similar ICT legal and policy measures in the FNDP and the National ICT policy. However, having good policies on paper is one thing and the implementation of such policies is yet another thing. The Government, should go beyond the initiation of better policies and facilitate their funding, monitoring and implementation.

---

[141] See Unit 7.2.2 of the FNDP.
[142] Unit 7.5 of the FNDP at p.68
[143] **See** Chapter 6.13.2(a) of the National ICT policy
[144] Unit 7.5 of the FNDP at p.68

3.3 The Millennium Development Goals

The Millennium Development Goals[145] (MDGs) are eight goals that 189 United Nations member states have agreed to try to achieve by the year 2015.[146] The MDGs were developed out of the eight chapters of the United Nations Millennium Declaration, signed in September 2000. Zambia is one of the countries that were represented at the millennium summit and has committed itself to the attainment of the MDG's. The eight goals are:

1. *Eradicate extreme poverty and hunger*
2. *Achieve universal primary education*
3. *Promote gender equality and empower women*
4. *Reduce child mortality*
5. *Improve maternal health*
6. *Combat HIV/AIDS, malaria, and other diseases*
7. *Ensure environmental sustainability*
8. *Develop a global partnership for development*

The attainment of these goals is bound to a successful ICT development. This is why countries that have harnessed the potential of Information and Communications Technologies (ICTs) have attained significant social and economic development. The UN membership, therefore, recognizes the role of ICTs in the social and economic development of the nations and the world at large and has emphasized the need to increase and improve access to ICT.

Although all other Goals would require the use of ICT's in their attainment, however, Goal 8 ; that is "Develop a global partnership for development" differs in form and substance from the others, focusing primarily on changes in the policies of nations and of international institutions – changes for which information and communication technologies (ICT) may not be very relevant. In most cases, the role of ICT is minimal compared to the attainment of Goal 8. The efforts highlighted within this Goal include improving access to ICT and new technologies. This requires more attention in respect of promoting non-abuse of technology by the adoption of appropriate legal and regulatory frameworks. The government of the Republic of Zambia has

[145] Hereinafter referred to as the MDG's
[146] Http//www.wikidedia.com/ visited: 21st October 2008.

acknowledged this in the ICT policy hence coming up with a number of cyber security measures as alluded to earlier in the discussion.

In summary, what must be borne in mind is that the well intended Millennium Development Goals require a safe cyber space both in their pursuit and sustenance. With the increasing use of information technology necessary in the attainment of the MDG's, cyber criminals are also seeking to further their criminal activities. Therefore, not having a well framed legal and regulatory regime to counter cybercrime would not only make the attainment of the MDG's more difficult but also undermine their perpetuation once they are attained.

3.4 Conclusion

The analysis of the National ICT policy and the FNDP shows consistency on the part of government's commitment towards the ICT sector. The two documents have indeed addressed most essential cyber security concerns and several guides for future legislative reform have been identified in these policy documents. The only major challenge is that of ensuring the prompt implementation of the policy goals. The urgency of implementing the ICT goals in the FNDP and the ICT policy is also necessitated by the need to promote ICT's so as to help in the attainment of the MDG's. The MDG's, particularly goal number eight that advocates for an increased use of ICT's further justify the development of a legal and regulatory framework that would ensure reduced abuse of ICT's.

CHAPTER FOUR

A CASE FOR NON-PENAL MEASURES IN THE FIGHT AGAINST CYBERCRIME

4.0 Introduction

This chapter looks at the formal statistics of cybercrime in Zambia and advocates for the employment of non-penal measures in the fight against cybercrime.

4.1 Cybercrime statistics in Zambia

In light of the ever increasing reliance on the use of ICT and computer technology there stands the need to have a look at the formal statistics about this type of crime for Zambia and try to give an analysis on whether the reported cases do reflect the actual level of computer crimes committed or experienced in the country.

A search for statistics at the Zambia Police Headquarters revealed that hardly any records exist for cybercrime due to non-reporting of the incidents. The author also had an opportunity to consider one cybercrime case that had gone to court. This is a case involving the former University of Zambia assistant registrar in charge of admissions and examinations James Chisenga who is being charged with unauthorised modification of records contrary to s.6 of the Computer Crimes and Misuse Act. The defendant is alleged to have made unauthorised alterations to results for six candidates in order to make them meet the minimum entry requirements for admission to the University. [147] At the time of writing, trial in this case was still underway.

A check was also conducted at the Money Laundering Unit of the Anti Corruption Commission which looks into cybercrime related to fraud and exposed that only a handful of cases have been reported and none of these have successfully been taken to court due to reasons mainly bordering on insufficienct evidence.[148]

[147] See *THE POST*, 19 January 2009 p.7

[148] An interview was conducted with Mr Chilaizya a Senior Operations Officer of the Money Laundering Unit.

The above exposition, may on one hand be taken to mean that cybercrime in the country is not a common crime. On the other hand, the absence of formal records may be construed to entail that cybercrime is a common but silent form of a crime. In arriving at a determination as to which of the above two scenarios is true, regard may be had to the research conducted a couple of years ago in Uganda entitled: *Cyber Crime in Uganda: Myth or Reality?*[149] Though the research focused on Uganda, it may still be helpful in the Zambian scenario because the socio-economic setups of the two countries are not very distinct. By 2004, the nationwide population of Uganda's Internet users was 125,000.[150] Despite this number of internet users in Uganda being higher than that of Zambia i.e. still below 50,000 at present, the two countries are experiencing an increasing use of Information and Communications Technology (ICTs) in most aspects of life.

The study, aimed at investigating whether Internet users in Uganda have been victims or perpetrators of Internet crimes. The instruments used during the study included a web-based survey, telephone interviews, e-mail statements, face-to-face interviews, case studies and questionnaires. The participants consisted of students, researchers, the business community, community workers, law enforcement officers and lecturers. The sample space included institutions such as Universities, Government Ministries, internet cafes and media houses.

The study confirmed that most Internet users in Ugandan are both victims and perpetrators of Internet crime and all victims did not report to the police. The major cases involved intercountry situations including within Nigeria, Congo, Kenya and Canada. Over 90% reported to have been a victim of at least one cyber crime incident and twenty five percent confessed that they commit at least one wrongful act while in the cyberspace. The victims are mainly prey of spam, virus attacks and pornography, while the perpetrators are mostly spam senders, intellectual property infringers and hackers.

---

[149] F. Tushabe, and V. Baryamureeba *Cyber Crime in Uganda: Myth or Reality?* Proceedings of World Academy of Science, Engineering and Technology Vol.8 (October 2005)

[150] Britannica Encyclopedia : http://www.britannica.com/ ,visited on 17th August 2008

Despite the findings from the research, no formal records of cybercrime incidents were in existence in Uganda. The findings from the Ugandan study, can be logically be used to arrive at a conclusion that although there are no formal records in Zambia regarding cybercrime occurrences that does not mean no such mischievousness are committed. It may also be coherent to conclude that in Zambia, cybercrime is a common but silent crime because cases are not being reported. The gist therefore is to account for the unfortunate low or no records of cybercrime.

A number of reasons do exist why formal records of cybercrime are low. These may include the fact that many intrusion incidents go undetected due to poor conversance with technological advancements. Furthermore, when cybercrimes such as intrusions are detected, such incidents are barely reported to law enforcement and the reasons for failure to report may include fear of negative publicity or the fear of bestowing undue advantage to competitors.[151] Another factor is the nonexistent of a specific enforcement unit of the police to deal with cybercrime. In this connection some victims of cybercrime may feel relaxed to report incidents because of the thought that the ordinary police officers in Zambia are not vested with expert computer knowledge and cannot properly investigate or offer a solution to their problems. It is the authors' view that although a number of reasons account for the low formal record of cybercrime, one of the major issues to be addressed stand to be the poor level of awareness which the people of Zambia have in relation to the law on cybercrime. Raising the awareness levels in the country about the cyber laws would provide a great deal of strength to the deterrent effects of a criminal enforcement scheme.

4.2 Employment of non penal measures in the fight against cybercrime

4.2.0 Background

There are two ways of logically dealing with crime: reacting to completed crimes and preventing crimes before they are committed. However, the use of a proactive approach in

[151] A. Purugganan, 'Philippines cybersecurity update: laws, cases &other legal issues' in Reich, Pauline C (ed) *Cybercrime and security* (New York: Oceana Publications, 2006) p. 43

fighting cybercrime is seen as an advantageous and favorable model. The enquiry into non-penal responses to cybercrime is supported by several factors such as the level of reported cybercrimes which not corresponding to the actual perpetration. The fast changes in the advancement of technology, also makes it difficult for criminal law to be able to adequately cover such developments without legislative intervention which usually takes a long time to come forth. Furthermore, the problem of anonymity, jurisdictional issues, and the lack of resources in the law enforcement sector, also justify the focus beyond criminal law enforcement. A number of supplementary avenues may thus be explored in fighting cybercrime. These include technological measures, administrative measures and the employment of civil remedies.

4.2.1 Technological measures

The case for using technological measures in fighting cybercrime is mainly supported by an explanation that cybercrime may have unforeseen consequences capable of adversely affecting the entire world economic and social well being. Here, cybercrime may be prevented by using technological devices that are less susceptible to cyber interference. Updating technological tools and anti-virus software may help a great deal in combating cybercrimes such as hacking, password thefts as well as other system intrusion crimes. A cited example of how technological measures and developments can cushion the impact of cybercrime is the assessment that the *Melissa* virus of March 1999 that infected 1.2 million computers, including one in five businesses, causing $80 million in damages worldwide, would only have infected less than a quarter of the infected computers had the owners been using the best available firewall and antivirus systems at the time.[152] Similarly, it has been said by experts that the recent hacking of ZAMNET which is zamba's leading ISP by a notorious group of hackers known as the 3RqU Turkish would have been avoided if the servers were updated. [153]

---

[152] J.M. Schwarz, 'A case of identity': a gaping hole in the chain of evidence of cyber-crime. Boston University Journal of Science and Technology Law 9 (2003) 92.

[153] See Lusaka Times 'Zambia's leading ISP hacked', December 27, 2008 , derived from; http://www. lusakatimes.com (Accessed: December 27, 2008)

4.2.2 Administrative measures

Having good administrative measures and policies in organizations and institutions that use computer technology may is yet another proactive response the cybercrime menace. For example, it was confirmed that the recent ZAMNET hacking incident would not have occurred but for the lax in ZAMNETs policy on applying security updates to the software on their servers.[154] Administrative regulations may thus see to it that the personnel using various ICT tools are made to develop better habits that would mitigate the levels of cybercrime attacks. Personnel may be made to bear responsibility for the ensuring that software security in regularly updated. Furthermore, downloading of 'unknown' programmes form the internet may be made a subject of scrutiny by specialized IT experts. Furthermore, having well qualified IT experts in the firm or organization would help in the detection of possible weak points in the computer systems. Similarly, keeping the workforce abreast with the IT skills as well as the cyber laws would help a great deal in reducing the abuse of technology. And since in reality, most cybercriminals are employees, ex-employees, or other insiders who exploit their knowledge of corporate computer networks, many cybercrimes could be prevented through the use of better password controls and employee training and screening.[155]

4.2.3 Civil remedies

In light of the possible repercussions of cybercrime, any avenue that consolidates its eradication should be welcomed and encouraged. The approach of pursuing civil remedies for cybercrime under the law of torts is among such measures that would offer remarkable help in the cybercrime arena. It must be mentioned at this juncture that the Computer Crimes and Misuse Act[156] does allow the award of civil remedies in addition to the criminal sanctions that may be imposed.[157]

---

[154] ibid

[155] [155] A.B. Robin., *Deterring the Spread of Viruses On-line: Can Tort Law Tighten the 'Net'?*, REV. LITIG 17 (1998) 343, 366 .

[156] Act No. 13 of 2004

[157] S.15(2)

Proponents of a tort law framework cite the inadequacies of law enforcement agencies to identify, locate and prosecute cyber criminals coupled with the rapidly developing infrastructure and judicial conundrums of cyberspace. Several computer mischievousness can be addressed through the law of tort as the foregoing discussion will show.

Actions for the tort of trespass to chattels may be useful for system intrusions. A trespass to chattels occurs when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization.[158] Trespass to chattels is actionable only if the defendant dispossesses chattels belonging to another and the chattel is impaired as to its condition, quality, or value. This tort is triggered when the possessor is deprived of the use of the chattel for a substantial period of time. Thus the sending of unsolicited emails may fall under this tort. The case illustrating this is **CompuServe, Inc. v. Cyber Promotions, Inc.**[159], in which an ex-employee of Intel Corporation was found to have committed trespass to chattels by sending thousands of e-mails to current employees of the company. This case illustrates that Spamming" i.e. the practice of sending unsolicited or unwanted mail in an indiscriminate fashion may amount to trespass to chattels.

The distribution of viruses may also be actionable tortuously. A company that knowingly distributes infected computer software might be held liable for fraud or misrepresentation. The introduction of a computer virus might also constitute conversion or trespass to chattels.[160]

Furtthermore, a company that has failed to use antiviral software might be liable based on a negligence theory. Consequently, tort liability for Internet security violations may probably result in greater investments in computer security to protect our most critical assets from cybercriminals.

Civil remedies have been viewed to be a more viable legal solution to cybercrime especially in cases against an enterprise than criminal prosecution. Tort law (specifically the tort of

---

[158] B.A. Garner, A Dictionary of Modern Legal Usage (2d ed. 1995), 995

[159] 962 F. (S.D. Ohio 1997).

[160] A.B. Robin., *Deterring the Spread of Viruses On-line: Can Tort Law Tighten the 'Net'?*, REV. LITIG 17 (1998) 343, 366 .

negligence) is likely to pressure large market sectors such as Internet service providers (ISPs) to adopt security measures that prevent cyber criminals from plying their trade and more readily identifies them.[161] Using our ZAMNET example, the owners of websites that were for sometime off-line due to the hacking, could bring an action for negligence against ZAMNET since the root cause was that the security software on servers were not upto date.[162]

From a victim's perspective, the rationale for pursuing civil rather than criminal remedies offer advantages such as confidentiality, standard of proof that does not require evidence 'beyond reasonable doubt' and a more timely settlement for compensation. Another advantage is corporate liability. The victim doesn't have to identify a particular individual as the individual hacker since a corporation can be liable for damages either vicariously or through contributory negligence; this also provides the claimant with the ability to access significant damages.

4.3 Conclusion

This chapter has examined and considered the formal record of cybercrime in Zambia and it has been revealed that the statistics do not reflect the actual levels of crimes. Several reasons have been cited for this position which include the lack of awareness of cyber laws, fear of negative publicity and fear of bestowing undue advantage to competitors. The absence of an established unit of the police to deal with the crime also makes victims relaxed to report crime such as intrusions. It has also been argued in this chapter while citing appropriate examples, that the impacts of cybercrime may be fatal and law enforcement should not be the only solution to cybercrime and that the spectrum of solutions should be enlarged. Technological and administrative measures as well as the pursuit of civil remedies have been identified as having the ability to consolidate the cybercrime eradication effort.

[161] As per Ajoy Ghosh (IT security consultant and forensics expert) derived from; http://www.securitynewsportal.com (Accessed: 25/09/08)

[162] The websites that were affected include those of the State House, Bank of Zambia and Zambia National Broadcasting Corporation.

CHAPTER 5

AN ASSESSMENT OF REGIONAL AND INTERNATIONAL EFFORTS ON CYBERCRIME

5.0 Introduction

This chapter primarily examines the avenues available to Zambia in dealing with cybercrime beyond its borders. In this regard, an examination of regional efforts by SADC and COMESA regional bodies is made.[163] At international level, particular attention is given to the Council of Europe Convention on Cybercrime (2001), highlighting its merits as well as the main concerns that have been raised against it.[164] The enquiry into regional and international efforts is justified because cybercrime is transnational in nature in that it may be perpetrated from anywhere in the world. Thus, a nation cannot adequately fight cybercrime solely by the adoption of legislation criminalizing cyber offenses. Effort is needed to coordinate national responses both in terms of specifying offences and in applying the laws that are enacted to cross-border illegal acts. Without measures that actively coordinate national actions and policies at the international level, the amalgam of national cyber laws and policies is unlikely to result in a coherent framework for the identification, investigation, and prosecution of computer crimes occurring within or affecting multiple jurisdictions.[165]

5.1 Regional efforts

5.1.1 SADC

At SADC, the realization of the benefits of technology through the use of ICT is much advocated. However, the SADC member states have also acknowledged that in order to fully benefit from ICT's, there is need to focus on creating the requisite harmonized policy environment, as well as legal and regulatory frameworks to promote ICT diffusion and use.[166] It is from this background that the SADC membership developed the SADC model legislative

---

[163] Zambia has membership of both SADC and COMESA bodies.

[164] The Council of Europe Convention on Cybercrime (2001) is the most significant international effort in the cybercrime eradication arena warranting special consideration.

[165] T. L. Putnam and D. Elliott *International Responses to Cyber Crime,* (Hoover Press, 2006), p.52

[166] See Chapter 4.6 of the Regional Indicative Strategic Development Plan.(2006), p.60

provisions (MLP) or guidelines on pertinent ICT issues to clearly define the digital landscape. Although the model legislative provisions does not specifically address the cybercrime concerns, Members of SADC are taking initiatives to introduce and place into context the requirement and prerequisites of Cyber legislation and harmonization with the region. For instance, in 2005, SADC called for a meeting in Mbabane, Swaziland whose theme was 'CyberLaw Development and Harmonisation within SADC'. Three major outcomes of the meeting were: (a) that independently of the issue of harmonization, SADC countries need to mobilize their efforts to adapt their legal frameworks for the new technologies. (b) that the SADC countries should work together towards harmonization of the national laws, through ways such as the development of a SADC Web-based portal to facilitate best-practice dissemination and regional networking in this domain. (c) that member states should introduce capacity-building programmes for the judiciary, magistrates and police prosecutors, with a focus on proper methods of collecting, preserving and presenting admissible evidence in cases involving computers and computer data.[167]

4.1.2 COMESA

COMESA has the cyber security concerns enunciated in the ICT policy. An ICT Policy and Model Bill for COMESA were adopted by the COMESA Policy Organs meetings in Khartoum, Sudan, March 2003. Member States are in the process of integrating them into their regulatory framework. ICT policy guidelines and strategies adopted up to now include interconnection, licensing, universal access competition and pricing and consumer protection. The ICT policy advocates for the adoption of appropriate legal and regulatory framework that would ensure and assure the safety of the cyber space.[168] The foregoing therefore shows that COMESA as a regional body just as the case with SADC, is also concerned with the cybercrime menace.

---

[167]See, Report on the Seminar held in Mbabane, Swaziland, 5-8th April, 2005 CESPAM EXECUTIVE TRAINING PROGRAMME *'CyberLaw Development and Harmonisation within SADC'* p.2

[168] See COMESA Policy Guidelines On Consumer Protection (2007) p.7

5.2 International efforts

5.2.1 United Nations

The United Nations has also done some work in their attempt to provide some solution to the problem of cybercrime. It has hosted more than eleven crime congresses so far and the issue of computer-related crimes often features on their agenda.[169] For example, in the Eighth United Nations Congress held in 1990 in Havana, Cuba, the Congress adopted a resolution on computer-related crime calling upon its member states to intensify their efforts to combat computer crime.[170] The UN also produced a Manual on the Prevention and Control of Computer-Related Crime in 1995, which examined the law governing such crime and the need for international cooperation in investigations. Workshops were likewise held in the tenth and eleventh congresses, with some focus on public-private sector cooperation and between countries. Even the UN General Assembly (UNGA) has addressed the issue. In December of 2000 the UNGA adopted Resolution 55/59, the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century, which committed member states to work towards enhancing their ability to prevent, investigate and prosecute computer-related crime.[171]

5.2.2 The G.8

The G8 has been formulating policy and action plans to deal with high-tech and computer-related crimes for about a decade now. In December 1997, representatives from the eight major industrialized nations forming the G8 adopted ten principles and agreed on a ten-point action plan to fight international computer-related crime. The leaders of the G8 countries endorsed this template and G8 experts forming the Subgroup on High-Tech Crime continue to meet regularly

---

[169] See the latest on the U.S. Congress at the UN Office on Drugs and Crime web site at: http://www.unodc.org/unodc/en/crime_cicp_congresses.html.

[170] *See, S.W. Brenner and J. Schwerha,* Transnational Evidence Gathering and Local Prosecution of International Cybercrime, *Marshall J. Computer & Info. 20 (2002). 347, 359*

[171] W. B. Chik, *Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore* (2004) p.32

to cooperate on the implementation of the action plan. The Subgroup was charged with the task of enhancing the abilities of G8 countries to prevent, investigate and prosecute crimes involving computers, networked communications, and other new technologies. They have also expanded their work with non-G8 countries in this respect. The Subgroup meetings are attended by multi-disciplinary delegations that include cyber crime experts, investigators and prosecutors. It is to be noted that as part of a holistic strategy, the Subgroup closely cooperates with private industries to achieve these ends.[172] The G8 has remained dedicated to the issue and to finding an international and concerted solution to the problem.[173]

5.2.3 INTERPOL

As the world's largest international police organization created to facilitate transnational police cooperation and other crime fighting organizations, INTERPOL has been concerned with the issue of cooperation in the field of computer-related crime[174] Among its many efforts, INTERPOL uses a network of regional working party group of experts consisting of representatives from national computer crime units.[175] INTERPOL has also held conferences with its Sixth International Conference on Computer Crime held in April 2005 in Cairo, Egypt, and its First International Cyber Crime Investigation Training Conference in September 2005 at the General Secretariat. INTERPOL also promotes cross-disciplinary support between the academia, private industry and the authorities.[176]

---

[172] See, J. T. Soma et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?* 34 Harv. J. on Legis. (1997). 317, 359-360

[173] See, S.W. Brenner and J. Schwerha, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime,* Marshall J. Computer & Info. 20 (2002) 364-365

[174] INTERPOL facilitates cooperation between national law enforcement agencies as they investigate multinational online crime.

[175] See the INTERPOL ITC web site at: http://www.interpol.int/Public/TechnologyCrime/default.asp. INTERPOL has also established a Steering Committee for Information Technology Crime, which coordinates and harmonizes the initiatives of the various working parties.

[176] W. B. Chik, *Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore* (2004) p.32

5.2.3 Council of Europe Convention on Cybercrime (2001)

5.2.3.0 A Brief overview

Main focus of the Council of Europe Convention on Cybercrime (2001) is to combat cyber-crime on an international scale, to unify the nations against computer crimes, and to harmonize laws universally regarding offense, prosecution, and punishment.[177] The Convention addresses substantive law, procedural law, and jurisdictional aspects for all signatory states.

Parties to the Convention agree to adopt penal legislation addressing five types of cybercrimes: (1) illegal interception of and/or interference with computer data, illegal access to and/or interference with computer systems, and the misuse of devices to commit any of these offenses; (2) computer-related forgery and fraud; (3) child pornography; (4) the infringement of copyright and related rights; and (5) provisions governing the imposition of aiding and abetting and corporate liability.[178] They would also agree to adopt legislation guaranteeing the availability of certain procedures used to investigate cybercrime and apprehend cybercriminals. The Convention further seeks to promote international cooperation by dealing with extradition[179], mutual assistance[180] between police forces and designated points of contact for computer crime issues. The complex matter of jurisdiction is also covered under the Convention.[181]

5.2.3.1 Potential benefits of the Convention for Zambia

As noted in the preceding chapters, Zambia is heavily becoming dependent on computers that are networked, and this offers many cybercrime targets across every sector of society. Left unchallenged, cybercrime poses a serious threat to the health and safety of our citizens, and may stifle the Internet's power as a tool to communicate, engage in commerce, and expand people's

[177] See the Preamble to the Convention

[178] See Articles 2-11

[179] Article 24 deals with extradition of criminals between member countries. "The obligation to extradite applies only to" those crimes committed in Articles 2 to 11. Furthermore, the Article, enacts that extradition can only be sought where the maximum penalty is at least one year in jail

[180] Article 23 advocates mutual assistance among member states including in matters such as the collection of data and evidence in electronic form for the criminal offense.

[181] Under section 3 of the Convention, Signatories must establish jurisdiction over any offense via legislative or any other necessary means. Such jurisdiction will apply when the offense is committed in the territory of the signatory's country, on board a ship of the signatory, on board an aircraft of the signatory, or by one of the signatory's nationals, "unless another state has territorial jurisdiction."

educational opportunities around the globe.[182] Thus, a country like Zambia, has much to gain from the Convention that is a strong, well-crafted multilateral instrument that removes or minimizes the many procedural and jurisdictional obstacles that can delay or endanger international investigations and prosecutions of cybercrime. The Convention several important aspects make the Convention a viable route to deal with cybercrime at international level. Firstly, is the requirement that signatory countries establish certain substantive offenses in the area of computer crime. Secondly, the convention also requires parties to adopt domestic procedural laws to investigate computer crimes and thirdly, the importance of the Convention lies in its provision a solid basis for international law enforcement cooperation in combating crime committed through computer systems.

If Zambia were to become a party to this Convention, it would directly benefit by having better methods of obtaining international assistance from other parties in computer-related crime cases, particularly because the other parties to the Convention would have similar minimum definitions of computer crimes and the domestic procedural tools needed to investigate those crimes.

5.2.3.2 Major concerns about the Convention

Several concerns have been advanced on the viability of the Convention in the fight against cybercrime. However, this section only looks at the main concerns that have been levelled.

5.2.3.2.1 ISP mandatory requirement to retain records of their customers' activity

One the most controversial issues in the Convention are the provisions that require Internet Service Providers to retain records regarding the activities of their customers.[183] According to Global Internet Liberty Campaign[184], these provisions pose a significant risk to the privacy and human rights of Internet users.

However, the Computer Hacking and Intellectual Property section of the FBI has strongly rejected the critics and has argued that first, it is important to distinguish between data retention

[182] C. J. Magnin, *The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?* (2001) p.48

[183] Articles 17, 18, 24, 25

[184] Global Internet Liberty Campaign, *Member Letter on Council of Europe Convention on Cyber-crime,* [http://www.gilc.org/privacy/coe-letter-1000.html] accessed: October 18th 2008

requirements, which would require providers to collect and keep all or a large portion of a provider's traffic as a routine matter, and preservation requirements, which enable law enforcement authorities, during the course of a criminal investigation, to instruct a service provider to set aside specified data that is already in the service provider's possession". Therefore, the U.S. Government agency asserts that there is no data retention in the Convention; there is, however, data preservation provision. Divergent views have been expressed and this has remained the most controversial part of the Convention. In fact, this concern itself could prevent some countries who will vote on the matter, to ultimately ratify the Convention.

5.2.3.2.2 Lack of dual criminality provision

The lack of a dual criminality provision, where extradition or international cooperation is concerned, can put a burden on Internet Service Providers (ISPs). Under the Convention, ISPs of one country could be forced to respond to requests on matters that are not illegal in another country. A cited example is hate speech. An ISP could be forced to hand over information about a customer to German authorities, while in the U.S. the customer is protected by the First Amendment to the U.S. constitution.[185]

5.2.3.2.3 Too large definition of "Illegal devices" in Article 6

The conception of "Illegal Devices" set out in Article 6 lacks sufficient specificity to ensure that it will not become an all-purpose basis to investigate individuals engaged in computer-related activity that is completely lawful. Technical experts have made clear that this provision will also discourage the development of new security tools and give government an improper role in policing scientific innovation.[186]

5.2.3.2.4 No provision exempting Service Providers for potential criminal liability

It has been asserted that the criminal provisions of Articles 9 and 11 could lead to a chilling effect on the free flow of information and ideas. Imposing liability on Internet Service Providers for third party content places an unreasonable burden on providers of new network services and will encourage inappropriate monitoring of private communications.[187] Furthermore, Service

[185] C.J. Magnin, *The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?* (2001) p.62

[186] It must be noted though that paragraph 2 of the Article 6 makes clear that legitimate scientific research and system security practices, for example, are not criminal under the Article.

[187] Supra note 22, p.63

Providers have expressed high concern that they might be held criminally liable for failing to monitor customer or user content, or for the criminal actions of their employees. An argument to the contrary has also been advanced that it is only when a provider becomes specifically aware that its system is being used to transmit or store criminal content, instructions, etc., that questions of liability may arise.[188]

5.2.3.2.5 International Cooperation and Investigative Procedures defined too vaguely

Critics believe that clear procedures must be agreed upon in international investigations, and that no law enforcement agency within a different jurisdiction should act on behalf of another nation without clear investigative procedures within its own jurisdiction.[189] They are concerned for the consistency of individual rights protections. I think personally that they are right. International investigations can not work in practice if the investigative procedures are not clearly defined and the Convention is not going far enough in this matter.

5.3 Conclusion

This chapter has highlighted the more prominent efforts that are being taken at the regional and international level in an attempt to improve the global crime-fighting regime against the advent of technological abuse. Even though they remain largely political and informal cooperative vehicles, they are no less instrumental and important as they reflect political commitment, international policy and consensus.[190] The European Convention on Cybercrime is one notable international initiative in the fight against cybercrime and despite the concerns that have been raised, the convention still has vast advantages outweighing the demerits. Zambia therefore should be part of such progressive initiatives and be seen to take appropriate measures at home to help realize and meet the international standards.

---

[188] T. L. Putnam and D. Elliott *International Responses to Cyber Crime,* (Hoover Press, 2006), p.52

[189] C. J. Magnin, *The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space? (*2001) p.62

[190] See, S.W. Brenner and J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. Marshall J. Computer & Info. (2002) 347

CHAPTER SIX

RECOMMENDATIONS AND CONCLUSIONS.

This is the concluding chapter of the dissertation and provides the recommendations and conclusions as set out below.

6.1 Conclusions

The first chapter covered the introductory aspects. The second chapter undertook a comparative analysis of Zambia's legislative responses to the challenges of cybercrime with the approaches in other jurisdictions. Although Zambia took a right step in putting in place cybercrime specific legislation on the statute book, several aspects have been identified to be lacking in our laws. Furthermore the chapter highlighted that the traditional legislation that may be relevant in regulating cybercrime has unfortunetly remained couched in archaic wording thereby requiring amendments to properly apply in this electronic setting. The chapter concluded by showing how inadequate the Law in Zambia is with regard to governing commercial transactions conducted via the electronic frontier. The rise in electronic commercial transactions has been seen to urgently require an appropriate legal framework which unfortunately is lacking in Zambia.

Chapter three looked at Zambia's policy aspects in ensuring safety on the cyberspace. An analysis of the National ICT policy showed vast measures that the government intends to implement which would positively help in promoting cyber security and safety in the use of ICT's . Therefore the various issues raised in the policy would greatly consolidate cybercrime prevention and eradication efforts if they are implemented. The chapter also looked at the Fifth National Development Plan (2006-2010) which was launched before the ICT policy (2007) came into being and has shown that most of the important issues relating to cyber security and safety and non abuse of technology are also enunciated in the FNDP which in itself reflects a high level of consistency on the part of the Government. The chapter has also shown that the

Fifth National Development Plan (2006-2010) has given fair attention to the ICT sector which relates well to the implementation of the National ICT policy. The chapter ended by looking at how the urgency in implementing the ICT goals in both the FNDP and the ICT policy is much necessitated by the need to promote ICT's so as to help in the attainment of the MDG's. The MDG's, particularly goal number eight that advocates for an increased use of ICT's has further been seen as justifying the development and implementation of a legal and regulatory framework that would ensure reduced abuse of ICT's.

Chapter four looked at the formal records of cybercrime offences and advocates for the employment of non criminal measures in the fight against cybercrime. It has been argued in the chapter that the absence of statistics on cybercrime in Zambia, does not in any way mean that such crimes are not perpetrated. Several reasons have also been advanced for the poor formal statistics of cybercrime as well as how the situation may be ameliorated. Lastly the chapter looked at the feasibility of employing non-penal measures in the fight against cybercrime. A proactive and not reactive approach has been advocated in view of the devastating impacts that cybercrime may inflict and the use of non penal measures has been seen to be one of the important efforts that may be promoted on the electronic frontier. Several non penal measures such a technological and regulatory measures have thus been advanced. It has further been advanced that the non regulation of the IT professionals in the country possess a challenge of compromising safety on the electronic frontier.

An assessment of the regional and international efforts in the fight against cybercrime was the main theme of chapter 5. The chapter looked at the efforts at the SADC and COMESA regional bodies and showed a fair but developing commitment on the subject. The seriousness of the cybercrime menace has also been exhibited through the measures that the UN, the G8, and

INTERPOL have been undertaking in fight against cybercrime. The chapter reveals that Zambia has not do enough to deal with cybercrime at transnational level and wraps up by looking at the first and major international caucus on cybercrime: the Council of Europe Convention on Cybercrime which came into force more than 8 years ago, highlighting the potential benefits as well as the major concerns that have been raised against the convention. The study espouses that the advantages of Zambia being party to the convention do outweigh the possible demerits of such a development.

6.2 Recommendations

(i) The comparative law analysis with several jurisdictions revealed that the Zambia still lacks behind in combating cybercrime owing to non criminalisation of certain serious cybercrimes. The following offences should therefore be criminalised:

a) Identity theft

b) Manufacture of devices for purposes of furthering the commission of cybercrimes

c) The sending of unsolicited electronic mail.

(ii) The present three years maximum sentences for the offences of unauthorized access and unauthorized modification do not send a good message to would-be offenders and cannot be appropriate in punishing criminal activities such as hacking. This therefore requires revision by the legislature. The proposed sentences are;

(a) Maximum sentence for unauthorised access be increased from the present three years to five years, while in case of a subsequent offence, the current 5 years maximum sentence should be increased to 10 years.

(b) Maximum sentence for unauthorised modification be increase from the current three years to five years.

(iii) Zambia's legal regime as seen in the discussion, has not taken into account the inadequacy of traditional legislation is to tackle technologically perpertrated conventional crime. In this

regard, the following offences should be clearly legislated against with technological advancements in mind:

a) Computer related forgery
b) Computer related fraud
c) Theft
d) Ponography
e) Intellectual property rights infringement.

(iv) In view of the rapid changes in technological advancements, the legislature should never neglect the tenet of ensuring that legislation is drafted in a technologically neutral manner.

(v) In light of the increased use of ICT's in the country as well as the booming of electronic commercial transactions, there is urgent need for an appropriate legal framework that would govern electronic commercial transactions and clearly lay down the rules and regulations of contract law that should be taken in an electronic setting. Zambia may draw from approaches taken by South Africa.

(vi) Alive to the fact that having laws is one thing while enforcing them is yet another, there is urgent need that the enforcement wing be established within the present law enforcement system which would be able to tackle cybercrime investigations and prosecutions. In this regard, there is need to provide the necessary support in terms of finances, human resource as well as appropriate training.

(vii) In light of the non-existence of the a body to promote professionalism in the ICT sector, it is recommended that measures be undertaken to either create a new body or empower the Computer Society of Zambia with appropriate powers to enable the registration, regulation and disciplining of IT professionals in Zambia.

(viii) It is recommended that there is need to educate the citizenry on the cyberlaws in Zambia through such means as the provision of educational materials for example, which explains the scope of the Computer Crimes and Misuse Act. Such measures, will provide a valuable resource

for others to refer to, will reassure the public, and will perhaps even discourage potential miscreants. Above all, educating the citizens would go a great deal in reducing the difference that has been seen to exist between formal records and the actual perpetrated computer crimes.

(ix) It is recommended that the Government address the lack of statistics on cybercrime by means of small-scale statistical sampling, because without good figures on the scale of cybercrime activity, policy formation is unnecessarily difficult.

(x) It is recommended that the use of preventive approaches such as administrative measures and technological tools be encouraged in the fight against cybercrime in light of the challenges of a reactive approach to cybercrime. It thus further recommended that the ISP industry develop Best Practice procedures for proactive monitoring of the security of their customers' machines.

(xi) It is recommended that the Government avoids any further unnecessary delay and move swiftly to ratify the Council of Europe Convention on Cybercrime. This is in light of the transnational nature of cybercrime which makes it difficult to be dealt with by an individual country without international co-operation.

(xii) It is further recommended that owing to the transnational nature of cybercrime and the need for international co-operation, Zambia must go further than just being part of regional and international efforts by providing the necessary political will and leadership at home especially in implementing its regional and international commitments.

(xiii) It is also recommended that the government adheres and implements its commitments in the FNDP and the ICT policy vis a vis promoting safety on the electronic frontier especially that the speedy attainment and possible sustenance of the MDG's is largely dependent on a reduced abuse of computer technology.

BIBLIOGRAPHY

BOOKS

David I Bainbridge Introduction to Computer Law, Oxford: Blackwell , 2000

Garner, B.A. *A Dictionary of Modern Legal Usage* (2nd ed), New York: Vintage, 1995

Harris, D.J. *"Cases and Materials on International Law"*, London: Sweet & Maxwell, 2003

Marjie, B. *Computer Forensics and Cyber Crime: An Introduction.* New Jersey: Pearson Prentice Hall, 2004

Kanja G, *Intellectual Property Law,* UNZA Press, 2006.

Purugganan, A. A'Philippines cybersecurity update: laws, cases &other legal issues' in Reich, Pauline C (ed) *Cybercrime and security* New York, Oceana Publications, 2006

Putnam, T. L. and Elliott, D. *International Responses to Cyber Crime,* Hoover Press, 2006

Scambray J. *Hacking exposed,* London: Phoenix , 2001

CASES

R v Absalon [1979] 68 Cr App R 183
Entores v Miles Far East Corp [1955] 2 QB 327
Brinkibon v Stahag Stahl [1983] 2 AC 34.
CompuServe, Inc. v. Cyber Promotions, Inc. 962 [S.D. Ohio 1997]

INTERNATIONAL INSTRUMENTS AND CONVENTIONS

The Council of Europe Convention on cybercrime (2001).

SADC Regional Indicative Strategic Development Plan (2006)

COMESA Policy Guidelines on Consumer Protection (2007)

UNCITRAL Model Law on Electronic Commerce

JOURNALS/ARTICLES

J. T. Soma et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?* (1997) 34 Harv. J. on Legis..

E. Moustakas, C. Ranganathan & P. Duquenoy, *Combating Spam Through Legislation: A Comparative Analysis of US And European Approaches* (2006)

Edwards, Savage & Walden (editors) Information Technology & The Law (1990) 150.
Darryl C Wilson *Viewing Computer Crime: Where does the systems error really exist?* (1991) Computer Law Journal Vol. XI

Florence Tushabe, and Venansius Baryamureeba (2005) *Cyber Crime in Uganda: Myth or Reality?* Proceedings of World Academy of Science, Engineering and Technology Volume 8 October 2005

Michael Hirst *Cyberobscenity and the Ambit of English Criminal Law* (2002) Computers & Law Vol. 13 Issue 2

Mike Keyser, *The Council Of Europe Convention On Cybercrime* , Journal of Transnational Law & Policy (2003) Vol. 12*(2)*

Robin A. Brooks, *Deterring the Spread of Viruses On-line: Can Tort Law Tighten the 'Net'?*, (1998).17 REV. LITIG.

Schwarz, Joel Michael *'A case of identity': a gaping hole in the chain of evidence of cyber-crime* (2003) 9 Boston University Journal of Science and Technology Law.

S.W. Brenner and J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, (2002) 20 J. Marshall J. Computer & Info.

Susan W. Brenner *'Cybercrime investigation and prosecution: the role of penal and procedural law'* (2001) Murdoch University Electronic Journal of Law, vol. 8(2)..

W. B. Chik, *Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore* (2004)

LEGISLATION

Can Spam Act of 2003 (U.S)
Copyright and Performers Rights Act Cap 406 of the Laws of Zambia
Copyright, Designs and Patents Act of 1988 (U.K)
Computer Crimes and Misuse Act No.13 of 2004 (Zambia)
Computer Crimes Act (1990) (U.K)
Criminal Justice and Public Order Act of 1994 (U.K)

Federal United States Code (U.S)
Films and Publications Act 65 of 1996 (South Africa)
Identity Cards Act 2006(U.K)
Identity Theft Penalty Enhancement Act of 2004, HR, 1731
Penal Code Act Cap 87 of the Laws of Zambia
Protection of Children Act of 1978 (U.K)
Sexual Offences Act of 2003(U.K)
Theft Act 1978 (as amended by the Theft Amendment Act (1996) (U.K)
The Delaware Code

NEWSPAPERS

Lusaka Times, December 27, 2008
Mail & Guardian Newspaper, July 29, 2004

OBLIGATORY ESSAYS

"The Effectiveness of the Computer Crimes and Misuse Act No. 13 of 2004 in combating cybercrime in Zambia", 2006 Obligatory Essay by Doris N. Kapumpa.

REPORTS

Daily Parliamentary Debates For The Third Session Of The Ninth Assembly, of Tuesday, 3rd August, (2004)

National Legislation Implementing the Convention on Cybercrime-Comparative analysis and good practice Draft paper (2008)

European Commission Report (2003)

Report on the Seminar held in Mbabane, Swaziland, 5-8th April, 2005 CESPAM Executive Training Programme *'CyberLaw Development and Harmonisation within SADC'*, (2005)

WEBSITES

Http://www.securitynewsportal.com
Http//www.wikidedia.com
Http://www.britannica.com
Http://www.parliament.govt.zm
Http://www.britannica.com
Http/www.coe.int
Http://www.unodc.org
Http://www.geocities.com.
Http://www. lusakatimes.com
Http://www.mg.co.za