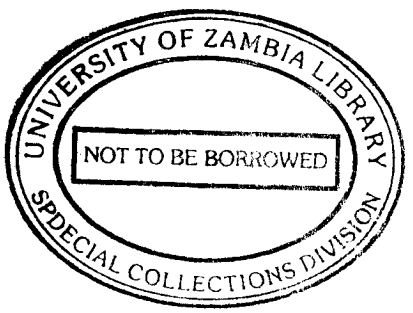
THE COMPUTER MISUSE AND CRIMES ACT 2004: ITS EFFECTIVENESS IN COMBATING CYBER CRIME IN ZAMBIA



By

DORIS NYIRENDA KAPUMBA

A paper presented in partial fulfilment of the requirements for the degree of Bachelor of Laws of the University of Zambia.

2006

DECLARATION

I, Doris Nyirenda Kapumba ,Computer Number 90119266 do hereby declare that the contents of this dissertation are based on my own findings. I further declare that the information used herein that is not my own I have endeavoured to acknowledge.

I, therefore declare that all errors and other shortcomings contained herein are my own.

..... 12-01-2007

Signature Date

UNIVERSITY OF ZAMBIA

SCHOOL OF LAW

I recommend that the obligatory essay prepared under my supervision by

DORIS NYIRENDA KAPUMBA

Entitled

THE COMPUTER MISUSE AND CRIMES ACT 2004: ITS EFFECTIVENESS IN COMBATING CYBER CRIME IN ZAMBIA

Be accepted for examination. I have checked it carefully and I am satisfied that it fulfils the requirements relating to format as laid down in the regulations governing obligatory essays.

Supervisor..... Date.....

Judge Kabazo Chanda

TABLE OF CONTENTS

DEDICATION

To my husband, Sipo, and children, Nonde and Mapalo, who had to forego so much to enable me realise my dream.

ACKNOWLEDGEMENTS

Heartfelt thanks go to my Supervisor, Judge Kabazo Chanda, for his well organised supervision and guidance.

Special thanks go to the Chief Parliamentary Legal Counsel in the Ministry of Justice, The Director of Information Technology and Communications in the Zambia Police Service and President of the Computer Society of Zambia for the invaluable assistance they rendered.

Last but not least, I wish to thank my employer, the National Assembly of Zambia, for the time and support I was given.

CHAPTER I

1.0 INTRODUCTION

1.1 HISTORICAL BACKGROUND

Crimes committed against computers or information on computers is a growing concern for most nations as its impact transcends all sectors of society. Undeterred by prospects of arrest or prosecution, cyber criminals threaten the financial health of businesses, the faith of their customers as well as national security.[1] Issues such as morality, privacy and the freedom to choose what information one should receive are also not exempt from the activities of these omnipresent criminals.

The fact that computer crime is able to lash at the very core of society, thus, threatening its very existence created a challenge for states as the existing laws in many countries around the world were unable to cater for cyber crimes. This prompted various states to put in place legislation criminalising various conduct. The international community also came up with conventions under which state parties were obliged to enact legislation to this effect.[2]

---

[1] www.mcconnellinternational.com 'Archaic laws Threaten Global Information' December 2000

[2] Judge S. Schjolberg and A. M. Hubbard, *Harmonising National Legal Approaches on Cybercrime* p.3

Two major events in Zambian history, one political and the other economic, led to the enactment of cyber crime legislation in form of the Computer Misuse and Crimes Act 2004.The first was the hacking of the State House Website which resulted in a caricature of the then President, Dr Frederick Chiluba, being posted on the Website. The culprit was apprehended and inappropriately charged with defamation of the president as per Section 69 of the Penal Code. As such, the case did not succeed.[3] What emerged from this incident, however, were the glaring inadequacies in the Zambian legal system with regard to computer crimes.

The second issue that led to the enactment of the Act was the frauds that had rocked banks and other financial institutions since the emergence of widespread use of computers and other high technological processes in banking and other financial institutions and the nation at large.

While the ensuing legislation satisfactorily helped forestall the frauds, it neglected to adequately address other areas. This situation was worsened by the highly dynamic nature of computer technology and crimes which entail that legislatures world over are proactive as new computer crimes emerge with more development in the industry.

For instance, at the time the Computer Misuse and Crimes Act 2004 was conceived, the use of the Internet was not as widespread and diverse as it is today. This was even less so in Zambia. As such, the law failed to adequately address issues such as unsolicited electronic mail or spam. Also conspicuously absent was the issue of pornography which

[3] www.cinsa.info Tisha Steyn,'Zambia to Fight Cyber Crime'

since the emergence of the Internet, has reached epidemic proportions. There was also a need for the law to have outlawed the development and manufacture, for unlawful purposes, of devices used in the commission of computer crimes.

Finally, the effectiveness of the Act is largely dependent on the availability of requisite enforcement mechanisms. Lack of these will render it impotent. This paper seeks to address these issues

1.2 DEFINING CYBER CRIME

Attempts have been made to define cyber crime and amongst them is that of D. L. Speer who says cyber crime refers to activities in which computers or other technologic equipment such as cellular phones are used to carry out unlawful activities like theft, fraud, electronic vandalism and violation of intellectual property rights.[4]Computer crime has also been said to refer to any crime connected with the abuse of computers and informatics systems in general.[5]

The United States of America Federal Bureau of Intelligence National Computer Crime Squad has defined it as crimes where the computer is a major factor in committing the criminal offence.[6]The Organisation for Economic Co-operation and Development (OECD) Recommendations of 1986.defined computer related crime as any illegal, unethical or unauthorised behaviour relating to the automatic processing and transmission

---

[4] Speer DL92000) Redefining Borders: The Challenge of Cyber Crime *Crime Law and Social Change* Vol. 34, 259-273

[5] www.dataprotection 2003.info/Speakers/Maijan (site visited 09/06/06)

[6] www.cse.stanford.edu/class/cs201/projects98-99/computercrime (site visited 09/06/06)

of data.[7]The Council of Europe Recommendation of 1995 on Criminal Procedure defined it as any criminal offence in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer systems or electronic data processing systems.[8]

From the foregoing, it is clear that computer crime refers to any unauthorised attack on or usage of a computer which results in the commission of an offence and whose investigation may require access to computer systems.

1.3 CATEGORIES OF CYBER CRIME

Cyber crime can take various forms. For instance, the United States of America has classified cyber crimes into the following four major categories:[9]

Computer as a target of Crime

In this category, the computer itself is a target of vandalism and information theft. For instance, through the introduction of viruses.[10]

Computer as an Instrument of Crime

Here, a system, process or the data on a computer is modified to carry out an illegal act.

11

---

[7] Computer Related Criminality: Analysis of Legal Politics in the OECD (1986)
[8] Judge S. Schjolberg and A. M. Hubbard, *Harmonising National Legal Approaches on Cybercrime* p.3
[9] Speer DL92000) Redefining Borders: The Challenge of Cyber Crime *Crime Law and Social Change* Vol. 34, 259-273
[10] ibid

Computer as incidental to the Commission of another Crime

In this case, a computer is used to facilitate the commission of another crime. An example of this would be the distribution of child pornography over the Internet.[12]

Crimes Associated With the Prevalence of Computers

In this category the computer itself becomes the object of the crime. In this scenario, the crime involves the theft of computer hard ware or soft ware.[13]

1.4 TYPES OF CYBER CRIME

There is an array of computer crimes including the following:

- *Unauthorised access to computer systems or networks*
- *Theft of information contained in electronic form*
- *Email bombing* -this refers to sending large numbers of emails to the victim
- *Data diddling* – altering raw data just before a computer processes it and then changing it back after the processing is complete.
- *Salami attacks* – making alterations to data that are so small they almost go unnoticed. This is common in fraud in financial institutions. An example of this was in the *Ziegle*r case where an attack was carried out in which 10 cents was deducted from every account in a bank and deposited in a particular account.

---

[11] Ibid
[12] Speer DL92000) Redefining Borders: The Challenge of Cyber Crime Crime law and Social Change Vol. 34, 259-273
[13] Ibid

- *Denial of service attacks* – the computer of the victim is flooded with more requests than it can handle.
- *Virus/worm attacks* – Viruses attach themselves to a computer or file usually affecting the data on the computer. Worms don't need to attach themselves to the host, but make copies of themselves repeatedly until they eat up all the available space on the computer's memory.
- *Logic bombs* – These are event dependent programs. They are created to do something only when a certain event occurs.
- *Trojan attacks* – This is an unauthorised programme which gains control of another system by representing itself as an authorised programme.
- *Internet time thefts* – The Internet surfing hours of the victim are used by another. This is usually done by gaining access to their log in ID.
- *Web jacking* – In this crime, a hacker gains access and control over the Website of another. He may mutilate or change the information on the site.
- *Harassment via email* – this is similar to harassment through letters.
- *Cyber stalking* – following a person's movement on the Internet by, for example, posting messages on the bulletin boards frequented by them.
- *Internet Pornography* – the dissemination of pornography on the Internet.
- *Email spoofing* – misrepresenting the origins of an email.
- *Computer vandalism* – causing physical harm to a computer.
- *Intellectual property crimes* – Any act which deprives an owner of his rights. This includes software piracy, copyright infringement and trademark and service mark violations.

- *Cyber terrorism* – The use of the Internet to carry out terrorist attacks or other hate crimes.
- *Trafficking* – This can be human or drug trafficking.
- *Fraud and cheating* – These pertain to credit card and contractual crimes.[14]

1.5 LITERATURE REVIEW

To the best of my knowledge no study has been carried out on the Computer Misuse and Crimes Act 2004. Thus, this review will focus on the studies done prior to its enactment and highlight some of the recommendations that were omitted from the Act.

Cyber crime legislation has been evolving since the late 1970s during the early developmental stages of the Internet. The first comprehensive initiative being a study by the US Senate Government Operations Committee in February 1977.[15]

The study raised awareness of the potential dangers of unauthorised access to computer usage. Apart from that, it revealed that the US government had been hampered in its ability to prosecute computer crime because the laws had not kept abreast of changing computer technology.[16]

In Zambia, the Law Development Commission presented a report in 1998 highlighting the need for the country to enact computer misuse legislation. The report acknowledged

[14] http://www.naavi.org/pati/pati_cybercrimes_dec03htm (site visited on 16-10-06)
[15] Ibid p.4
[16] Judge S. Schjolberg and A. M. Hubbard, *Harmonising National Legal Approaches on Cybercrime* p.4

that while the widespread use of computers in commercial activities had yielded positive results such as an improvement in communications facilities and information flow, criminals had taken advantage of this new technology to commit more sophisticated crimes.[17]

While certain activities involving the misuse of computers were catered for by some of the provisions in the Penal Code, there were several computer related crimes which were not. For instance, the fact that a person attained a fraudulent advantage to the detriment of another through the manipulation of computer data posed a number of problems for the criminal law as it existed then.[18]

According to Cabinet Memorandum 03 (79) of December 2003, the following methods of dealing with the situation were considered:

1. *Maintaining the status quo* – This method was considered inappropriate as the severity of the problem needed to be addressed.

2. *Amending the Penal Code to Provide for Computer Fraud* – This was inappropriate because mere amendment of the Penal Code would not enable the inclusion of comprehensive computer crime provisions.

[17] Report on Computer Misuse Legislation, Zambia Law Development Commission, 1998, p 19
[18] ibid p.iv

3. *The enactment of separate legislation to deal with computer crimes* – This was the favoured and agreed upon method.

Because of the computer related financial frauds that had rocked the country and the difficulties encountered prosecuting computer fraud cases under existing legislation, the enactment of computer misuse legislation was spearheaded by the Bankers Association of Zambia[19] whose members had been the major victims of these fraudulent activities. The association not only commissioned the 1998 Law Development Commission Study on Computer Crimes, but also pushed for the enactment of the legislation between 1998 and 2004. Bearing this in mind, it is not very surprising that the Computer Misuse and Crimes Act of 2004 has a strong leaning towards electronic fraud and access to protected sites.

The Computer Society of Zambia in the Computer Misuse Bill Discussion Paper (2004) recommended that the Act include provisions proscribing the unlawful development of devices used in the commission of cyber crime. It also recommended the outlawing of indecent photographs or pseudo photographs. It further recommended that electronic evidence be made admissible.[20]However, these issues were conspicuously absent in the 2004 Act. Furthermore, when the Act was conceived and the study conducted, the country had not yet been exposed to the widespread use of the Internet. Consequently, Internet related offences may have been overlooked. Due to these factors, the Act appears to have some loopholes, hence, the need for this study.

---

[19] Bankers' Association correspondence to the Ministry of Communications and Transport, 4th June 2002
[20] http://cincsa.info/portal p.5 (site visited 08/06/06)

This study departs from previous studies in that it looks at the post enactment period and issues such as enforcement mechanisms and the new challenges created by the Internet which were not raised in the other studies.

This paper is divided into five chapters. The first introduces the study and gives a detailed background to the area of study and its significance. Chapter II is a detailed examination of the shortcomings of the Act. Chapter III examines computer misuse and crimes legislation in other jurisdictions such as South Africa, India, the United Kingdom, Australia and the United States of America as well as the Council of Europe Convention on Cyber Crime. Chapter IV provides a summary of the research findings and recommendations on how to strengthen the Act. The study culminates in Chapter V which is the conclusion of the paper.

CHAPTER II

2.0 SHORTCOMINGS OF THE COMPUTER MISUSE AND CRIMES ACT

2.1 UNSOLICITED ELECTRONIC MAIL OR SPAM

Before delving into whether the 2004 Act adequately provides for spam, there is need to define spam and to justify the enactment of anti-spam legislation.

2.1.1. Definition of Spam

With the advent of electronic mail, email, as a cheaper and quicker means of communication, has developed a phenomenon which has come to be known as spam.

Spam was born in Arizona in April 1994 when two Phoenix attorneys sent an advertisement to about 8,000 Usenet newsgroups. This advert reached over 20 million people and the angry response from these people crashed their Internet Service Provider's (ISP) computer. Since then, spam has grown from 8 per cent of all Internet traffic in 2001, to 56 per cent in 2003.[21]

To many, the term spam means nothing more than unwanted email. The two most common definitions of spam refer to unsolicited commercial email (UCE) and unsolicited

[21] Elizabeth A. Alongi, Has the US Canned Spam? Arizona Law Review Volume 46, 2004, p. 263

bulk email (UBE).[22]UCE is generally communication which has content of a commercial nature, for example, one that promotes the sale of a particular good or service. UBE, as the name connotes, refers to an email message which is sent in large quantities.[23]

The key aspect of nearly all definitions of spam is that the email must be unsolicited. Generally, a communication is considered unsolicited if there is no prior relationship between the sender and the recipient.[24]

2.1.2 Justification for Anti-spam Legislation

The issue of anti-spam legislation has generated a lot of debate with some arguing that spam, at worst, is nothing more than an irritation to the Internet user and, therefore, need not be legislated against. They further argue that after all, one can seek redress in tort either for nuisance or trespass to chattels. A further argument is that prohibiting spam would be a violation of the freedom of expression and would have serious ramifications on the advertising industry. However, the following reasons can be advanced to justify the necessity for anti-spam legislation.

Advertisers find spam an effective marketing tool because they can reach millions of potential clients at the cost of just one email. The downside of this, however, is that UCEs, have the effect of shifting advertising costs from the advertiser to the Internet

---

[22] David E. Sorkin Technical and Legal Approaches to Unsolicited Electronic Mail, University of San Francisco Law Review Volume 35 2001 p. 325
[23] ibid p.330
[24] Ibid p.328

Service Providers and, consequently, the Internet user. This cost shifting may result in increased costs to ISPs who may require bigger storage space to handle the much larger email traffic. Alternatively, they may have to invest in more spam filtering devices, which, in some cases, may even entail having an entire department to deal with spam[25]. This increased cost to the ISPs, in turn, translates to a cost to the Internet user through increased subscription fees. Thus, the Government, which has a duty to protect consumers, needs to move in, through legislation, to arrest the situation. Let the advertiser and not the Internet user pay the marketing cost for products.

Another problem with spam is that it tends to interfere with people's right to be left alone. Spammers send emails into people's private mail boxes without their consent. That is an interference with their right to be left alone. In *Rowan v The United States Post Office Department*[26] the court concluded that a mailer's right to communicate must stop at the mailbox of an unreceptive addressee and that not to uphold this would be tantamount to licensing a form of trespass. Spammers send emails to the mailboxes of unsuspecting Internet users without their consent. This is an interference with their right to be left alone.

Spam further has the negative tendency of exposing unsuspecting Internet users to obscene and objectionable materials.[27] For a country like Zambia which prohibits the conveying or possession of obscene materials, anti-spam legislation would contribute to the control of pornography.

---

[25] http://vjolt.student.virginia.edu/graphics/vol4/home_art4.html p.7/46(site visited 18/07/06)
[26] U.S. 728 (1970) p 397
[27] Eric Goldman, Where's the Bee? Dissecting Spam's Purported Harms, 2004, p.15

Anti-spam legislation would also help protect consumers from Internet fraud and deception. Because spammers often use deceptive and fraudulent practices to disguise the origin of their bulk mail, it is almost impossible for defrauded consumers to trace them. [28] Thus, anti-spam legislation must proscribe the use of fraudulent practices to disguise the origin of mail.

As regards the fact that those affected by spam have an action in tort, it is a notorious fact that litigation is expensive. In the USA, for instance, because the larger ISPs can afford litigation, spammers have begun targeting smaller service providers which cannot.[29] For Zambia, apart from the expense, litigation also usually drags on for years. It would, therefore, be more prudent to put in place legislation that will deter would be spammers.

Finally, the failure to address the issue of spam has the potential of turning Zambia into a haven for spammers. This may have very costly repercussions on Zambian ISPs which will have to invest heavily to circumvent the activities of the spammers. The possible failure of ISPs to handle the increased traffic caused by spamming could also have serious repercussions on Zambian businesses and organisations for which the Internet has become a major communication and information tool.

With all these negatives resulting from spam, any legislation that is to effectively address cyber crime needs to address the issue of spam.

---

[28] http://vjolt.student.virginia.edu/graphics/vol4/home_art4.html p. 8/46
[29] Elizabeth A. Alongi, Has the US Canned Spam? Arizona Law Review Volume 46, 2004, p. 269

2.1.3 Effectiveness of the Computer Misuse and Crimes Act 2004 in Addressing Spam

There are two provisions in the Act that attempt to address the issue of spam. The first is Section 8 that provides that a person who knowingly and without authority interferes with, interrupts, or obstructs the lawful use of a computer; or impedes or prevents access to or impairs the usefulness or effectiveness of any programme or data held in a computer or causes directly or indirectly a degradation, failure or other impairment of function of a computerised system or any part therefor commits an offence.

This provision seems to place emphasis on interference with the functioning of a computer. Thus, it would probably apply in a situation where the spam results in either the crashing of the ISP or an impediment to the accessing of data. However, spam that does not result in an interference with the functioning of a computer is not covered. Therefore, this provision does not cater for spam which does not necessarily impede the functioning of a computer, but nonetheless is an undesired invasion of one's mail box. With the vast majority of ISPs and end users investing in anti-spam filters, the likelihood of an ISP crashing or computer malfunctioning due to spam is much reduced. Thus, this provision will not adequately address the spam problem.

The second provision is Section 12 (1) which provides that any person who with requisite knowledge and intent engages in conduct which causes a computer to cease to function

permanently or temporarily and at the time the person engages in that conduct has knowledge that the conduct is unauthorised commits an offence.

This provision, like Section 8, can only apply in a situation where the spamming results in a computer ceasing to function. However, its application to spam would be even narrower than that of Section 8 because of the definition of "requisite intent" which according to Section 12 (2) (b) means intent to cause a computer to cease to function.

This means that for one to be susceptible to this section, they must have intent to cause the computer to cease to function. Evidently, a lot of spamming goes on for purposes such as advertising, soliciting for funds and a desire to defraud unsuspecting Internet users and not necessarily to cause a computer to cease to function. Thus, such spamming would be outside the purview of this section.

2.2 Failure to Provide for Pornography

A glaring omission in the Act is any provision relating to pornography. This is a matter of grave concern as the advent of the Internet has exacerbated the problem of pornography to proportions that have never been reached before. Thanks to the Internet, people can access obscene materials in their offices, homes and even on their mobile phones.

In a country such as Zambia which has prohibited pornography, the Internet has made a mockery of our anti-pornography laws as nobody seems to observe them anymore due to the policing nightmare the Internet has created.

It may be argued that the issue of pornography was not addressed by the Act because Section 177 of the Penal Code amply covers it. Therefore, there is need to analyse this provision to see whether it adequately covers Internet pornography. The Section provides as follows:

Obscene Matters or Things

(1) Any person who

(a) 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; or

(b) imports, conveys or exports, or causes to be imported conveyed or exported, any such matters or things, or in any manner whatsoever puts any of them in circulation; or

(c) carries on or takes part in any business, whether public or private, concerned with any such matters or things, or deals in any such matters or things in any manner whatsoever, or distributes any of them, or exhibits any of them publicly, or makes a business of lending any of them; or

(d) advertises or makes known by any means whatsoever with a view to assisting the circulation of or traffic in, any such matters or things, that a person is engaged in any of the acts referred to in this section, or advertises or makes known how, or from whom, any such matter can be procured either directly or indirectly; or

(e) publicly exhibits any indecent show or performance or any show or performance tending to corrupt morals is guilty of a misdemeanour and is liable to imprisonment for five years or a fine of nor less than fifteen thousand penalty units nor more than seventy-five thousand penalty units.

While this provision does provide for a wide range of offences regarding pornographic material, the reference in sub-section (a) to 'any object' seems to suggest that at the time the provision was made what was visualised was a concrete thing, for instance, a picture. This view seems to be supported by the reference to 'makes, produces and has in possession' in the same sub-section. Thus, at that time, the Legislature had not envisioned

a situation where a person could have access to pornographic material which was not necessarily an object and even less in his possession.

The Internet has made both these things possible. What are contained on the Internet are not necessarily objects, but images until and unless printed. Furthermore, a person accessing pornographic material on the Internet who has not downloaded or printed them, in my view, cannot be said to be in possession of the material.

Therefore, if we were to go by this provision, a person surfing the Internet from one pornographic site to another without downloading or printing anything is not committing any offence. Such a state of affairs is tantamount to legitimising pornography in the country. There is, therefore, need for the accessing of pornographic sites to be proscribed.

The Internet has also introduced a new phenomenon of the owner of the computer not necessarily being the perpetrator of the offence. For instance, in the case of Internet Cafés who would be penalised for the offence; the owner of the computer or user who, in some cases, may not even be traced? There was need for the Act to clarify this position.

Evidently, the provision in the Penal Code does not adequately address the issue of pornography on the Internet and who should be targeted. There is, therefore, need for a provision to this effect in the Computer Misuse and Crimes Act.

2.3 Development and Manufacture for Unlawful Purposes of Devices Used in the Commission of Computer Crimes

As the world clamps down on cyber criminals all over the globe, the criminals will look to jurisdictions with weaker laws to go and carry out their activities. It must be remembered that cyber criminals are mostly intelligent people who once one avenue is blocked quickly seek another.

Zambia, as a nation whose information technology industry is not yet advanced should guard against being a haven for unscrupulous individuals wishing to engage in the manufacture of computer hacking devices, viruses and other devices that can be used in the perpetration of computer crimes. This requires that our computer misuse law proscribe the development and manufacture of these devices for unlawful purposes. That way, we will not become prey to investors with sinister motives.

2.4 Lack of Enforcement Mechanisms.

Any law is not worth the paper it is written on if there are not sufficient mechanisms in place to ensure its enforcement.

Section 16 (3) of the Act provides for the search and seizure, by a police officer, of any computer, data, program, information, document or thing which is believed to be

evidence that an offence under the Act has been or is about to be committed. By virtue of this provision, electronic evidence can be collected and presented as evidence in court.

The question that arises is: Has the Police Service been adequately equipped to carry out this tall order? Do the police, first of all, have a computer crimes unit? If not, why has the Act not deemed it fit to provide for one? Secondly, has the Police Service got officers trained in, to begin with, information technology and, beyond that, cyber crimes? Furthermore, are the judges who are expected to make a decision on this electronic evidence well versed in computer technology and computer law? In the absence of personnel trained in computer crimes, the implementation of this Act will remain a pipe dream.

Another cardinal issue is that since by virtue of Section 16 electronic evidence can be collected and adduced as evidence in court, the Police Service should have sufficient and appropriate equipment to enable them collect this electronic evidence. These are some of the issues that must be addressed for this Act to be effective.

CHAPTER III

3.0 INSTITUTIONAL AND LEGAL FRAMEWORK FOR COMBATTING CYBER CRIME INTERNATIONALLY AND IN OTHER JURISDICTIONS

Cyberspace has developed tremendously since the 1990s and its impact on society has been so fast that the laws have lagged behind. This has created a field day for cyber criminals. To compound the problem, cyber crime transcends international borders. Thus, a cyber crime committed in one country, today, can have serious repercussions on the world economy. For instance, in May 2000, the 'I Love You' virus was unleashed in the Philippines on computers on the Internet. It affected hundreds of thousands of computers worldwide causing billions of US dollars to be lost.[30] This global nature of cyber crime means that a global approach is required to adequately tackle cyber crime. Efforts to do this have been made through international organisations such as the United Nations, the Council of Europe, the Group of Eight (the G-8) and the Common Wealth.

On the national level, to ensure that cyber crime is curbed, laws must be enacted with sufficient clarity and specificity and countries should not rely on vague interpretations of existing pieces of legislation. Today, various countries have enacted legislation to deal with specific cyber crimes. Further, resources must be invested in training of investigators and prosecutors as well as in research on new trends in this crime.

---

[30] Fighting Cyber Crime: Efforts by Federal Law Enforcement, June, 2001, page 101

This chapter, therefore, delves into the various measures taken internationally to combat cyber crime. In addition, it examines various laws enacted in other jurisdictions to combat specific cyber crimes and institutions established to deal with cyber crime in general.

3.1 INTERNATIONAL INITIATIVES

3.1.1 The United Nations

The United Nations General Assembly has passed a number of resolutions on the use of cyberspace. Of relevance to this paper are resolutions 55/63 of 4th December 2000 and 56/121 of 19th December 2001 on combating the criminal misuse of information technology.[31]

These resolutions addressed various ways states could strive to combat cyber crime. These include states ensuring that their laws and practices eliminate safe havens for cyber criminals. Other measures recommended were a co-ordinated effort in investigation and prosecution of cyber crimes and the legal protection of the confidentiality and integrity of data and computer systems from unauthorised impairment. It was further recommended that the criminal abuse of computers be penalised and that the legal system should allow the preservation of data and quick access to it in the investigation of cyber crimes.[32]

---

[31] Harmonising National Legal Approaches on Cybercrime, International Telecommunications Union, 2005, p 6

[32] ibid

3.1.2 The Council of Europe

Perhaps the most comprehensive initiative towards a global combating of cyber crime was carried out by the Council of Europe. This culminated in the adoption of The Council of Europe Convention on Cybercrime in 2001 which came into force in July, 2004. This convention is a historic milestone in the combating of cyber crime. By June 2005, it had been signed by thirty-seven states and ratified by ten. An additional protocol on acts of a racist or xenophobic nature committed through computer systems was made in 2003 and had been signed by twenty-two States by June 2005. This convention is the only legally binding multilateral instrument which specifically addresses computer related crime.

Chapter II of the Convention provides for computer crimes that state parties should criminalise at national level. These include illegal access[33],illegal interpretation[34], data interference[35], system interference[36], misuse of devices[37], computer related forgery[38], computer related fraud[39], offences related to child pornography[40], copyright infringement[41] and aiding and abetting.[42]

Of particular significance to this study are the provisions on the misuse of devices and child pornography.

---

[33] Council of Europe Convention on CybercrimeArticle 2
[34] Article 3
[35] Article 4
[36] Article 5
[37] Article 6
[38] Article 7
[39] Article 8
[40] Article 9
[41] Article 10
[42] Article 11

Article 6(1) of the Convention commits state parties to criminalise not only the distribution, but also the production of devices used in the commission of computer crimes which is a welcome move.

The Article provides as follows :

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
>
> (a) the production, sale, procurement for use, import, distribution or otherwise making available of:
>
> (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;
>
> (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5.

By requiring state parties to criminalise not only the sale, procurement and distribution of devices used in the commission of computer crimes, but also their production, this convention ensures that countries do not become safe havens for those engaged in the manufacture of these devices for unlawful purposes. This is in line with the UN General

Assembly Resolutions 55/63 of 2000 and 56/121 of 2001 that require state legislation to ensure that a safe haven is not created for cyber criminals.

With regard to child pornography, Article 9(1) of the Convention provides as follows:

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
>
> (a) producing child pornography for the purpose of its distribution through a computer system;
>
> (b) offering or making available child pornography through a computer system;
>
> (c) distributing or transmitting child pornography through a computer system;
>
> (d) procuring child pornography through a computer system for oneself or for another person; and
>
> (e) possessing child pornography

This Article clearly refers to state parties having a specific provision outlawing not only child pornography in general, but specifically computer related child pornography.

By ratifying or acceding to the Council of Europe Convention on Cybercrime, States agree to ensure that their domestic laws criminalise the conduct described in Chapter II of the convention. They also undertake to establish the necessary procedural tools to investigate and prosecute cyber crime.[43]

3.1.3 The Group of Eight (G-8)

In 1997 the Group of Eight (G-8) Countries, established the High Tech Crime Subgroup. They adopted ten principles in the combating of computer crime. Like the UN, the G-8 emphasised that there should be no safe havens for cyber criminals in the world.

In 2004, the G-8 encouraged states to adopt the legal standards contained in the Council of Europe Convention on Cyber Crime.[44]

3.1.4 The Commonwealth

In an attempt to harmonise computer-related criminal law in the Commonwealth, member states came up with a model law at the Conference of Ministers held in 2002. This is modelled on the Council of Europe Convention on Cybercrime

[43] Harmonising National Legal Approaches on Cybercrime, International Telecommunications Union, 2005, p 10
[44] ibid p 7

3.2 NATIONAL LEGISLATION WITH REGARD TO SPECIFIC OFFENCES

3.2.1 Unsolicited Electronic Mail/Spam

Countries have taken a different approach to dealing with the problem of spam. While some countries have opted to criminalise it, others have chosen to handle it as a civil matter. This study will give an overview of both approaches.

The United States of America

The United States of America is one of the countries that have criminalised spam. The legislation that deals with spam there is the CAN SPAM Act 2003. The rationale behind the Act was to curb spam which had become the choice method for those who wanted to distribute pornography, perpetrate fraudulent schemes and introduce viruses into personal and business computer systems.[45]

Section 5 (a) (1) of the CAN SPAM Act 2003 prohibits the transmission of a commercial email containing false or misleading information about its origins.

Section 5 (a) (3) requires that a commercial email have a return address

[45] CAN SPAM Act 117 STAT, 2706

Section 5 a (5) requires that a commercial email be clearly labelled as such. Further, it must have an opt-out clause to allow the recipient to decline to receive further emails from the sender.

Section 5 (b) (1) of this Act criminalises the harvesting of electronic email addresses without the authorisation of the owners.

Section 5 (d) 1 requires warning labels on commercial emails with sexually oriented material.

Failure for senders of commercial emails to abide by these provisions will attract criminal prosecution.

The Republic of South Africa

A country with anti-spam legislation closer to home is South Africa. Like the USA, South Africa has criminalised the sending of unsolicited commercial emails.

The legislation dealing with spam in South Africa is the Electronic Communications and Transactions Act, 2002. Section 45 (1) of the Act requires any person who sends unsolicited commercial communications to provide consumers with the source of the email as well as an opportunity to opt- out from receiving further emails from that source.

Sections 45 (3) and (4) make any person who contravenes Section 45 (1) liable to criminal sanctions under Section 89 (1) which provides as follows:

> A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding twelve months.

Australia

In Australia, the Spam Act 2003 regulates commercial email and other commercial electronic messages. This Act, like the American and South African Acts, proscribes the sending of unsolicited emails without the identification of the source and a functional unsubscribe facility to allow the recipient reject further emails (sections17 and18).

Like the American Act, it proscribes email address harvesting. Section 20 of the Act makes it an offence for someone to supply email address harvesting software or harvested address lists. Section 21 goes further to make the acquisition of email address harvesting software or harvested address lists an offence. This Act further extends liability in the cited provisions to those who aid, abet or counsel the commission of the offences.

It is worth noting that in Australia, unlike in South Africa and the USA, contravening anti-spam legislation attracts civil rather than criminal liability. For example, Section

17(7) prescribes a civil penalty for persons that send commercial email without including accurate information on the sender as well as how they can be contacted.

From the foregoing, it is evident that countries have recognised spam as a problem requiring specific legislation. What appears to differ is the approach in dealing with the problem. Some countries like the USA and South Africa have chosen to criminalise it while others like Australia have treated it as matter carrying civil penalties. The manner in which spam has been legislated against also appears to differ. While some countries like the USA and Australia have come up with legislation specifically for spam, others like South Africa have included it under computer misuse legislation.

3.2.2 Pornography

The focus in other jurisdictions as regards pornography has been largely on child pornography. This is largely due to the fact that in many Western jurisdictions, being in possession of or viewing adult pornography is not an offence. It is for this reason that even the Council of Europe Cybercrime Convention singles out child pornography.

The United Kingdom

The two statutes that regulate pornographic material in the UK are the Obscene Publications Act 1959 and 1964. [46]

Section 2(1) of the 1959 Act makes it an offence to publish an obscene article or have an obscene article for publication for gain. Section 1(3) of the Act makes it clear that the term 'article' also refers to items like computer discs. Since Internet pornography is transmitted by means other than computer discs, for example, by phone lines or through modems, it is unlikely that it was adequately covered by the 1959 Act. An amendment to the Criminal Justice and Public Order Act 1994 resulted in an amendment to the term 'publication'. This amendment enabled the electronic transmission of pornographic material to be covered, hence, dealing with the lacuna in the law.[47]

The main concern of legislators in the UK, however, is child pornography. The main Act dealing with this issue is the Child Pornography Act 1978. This Act was passed amid the growing concern about child pornography.[48]

Through an amendment to section 84 (4) of the Criminal Justice and Public Order Act 1994, the definition of photograph given in section 7(4) of the 1978 Protection of

[46] Yaman Akdeniz,Governance of Pornography and Child Pornography on the Global Internet: A Multilayered Approach, Edwards L and Waelde C eds, Law and the Internet: Regulating Cyberspace Hart Publishing 1997, p228
[47] ibid
[48] ibid7 p.229

Children Act was extended to included photographs in electronic data format. This meant that the law adequately covered Internet child pornography.

Under Section 160 of the Criminal Justice Act 1988, as amended by section 84 (4) of the Criminal Justice and Public Order Act, it is an offence for a person to have in his/her possession an indecent photograph or pseudo photograph of a child.

India

India has taken a hard line approach to Internet pornography in general. It has designated it an offence punishable with imprisonment and a fine. This is contained in the Information Technology Act 2000. Section 67 of the Act provides as follows:

Publishing of information which is obscene in electronic form

> Whoever publishes or transmits or causes to be published in the electronic form any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances to read, see or hear the matter contained or embodied in it shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and with fine which may extend to two lakh rupees.

What is worth noting in all the legislation reviewed is that none talks about making viewing an offence. This means that if a country's legislation is not solid enough to extend possession, as in the UK's case, to having the material on the computer hard disc, it would be difficult to charge one of possession. In addition, the vast majority of people do not store the pornography on their computers, but merely browse from one Website to another viewing it. Thus, to curb this scourge, viewing should also be legislated against. For example, in its model legislation on child pornography, the International Centre for Missing and Exploited Children has recommended that the downloading as well as viewing of child pornography images be criminalised.[49]

3.2.3 Development and Manufacture for Unlawful Purposes of Devices Used in the Commission of Computer Crimes

South Africa

Section 86(1) of the Electronic Communications and Transactions Act, 2002 makes it an offence for a person to unlawfully produce any device for the purposes of committing a cyber crime. This is in conformity with the requirements of the Council of Europe Cybercrime Convention. Consequently, it helps avoid a situation where people engage in the manufacture of computer hacking devices, viruses and other devices that can be used in the perpetration of computer crimes.

---

[49] Child Pornography: Model Legislation and Global Overview International Centre for Missing and Exploited Children, 2006, p.3

3.2.4 Enforcement Mechanisms

The United States of America

In an attempt to combat cyber crime the USA has put in place various intuitions for purposes of investigating, researching on and educating the public on cyber crime. Numerous resources have also been devoted to developing a cadre of investigators and forensic experts with the requisite skills for combating cyber crime. Both the Federal Bureau of Investigations (FBI) and the Secret Service have taken a lead in this.[50]

In 1991, the US Justice Department put in place the Computer Crime and Intellectual Property Section (CCIPS) to look into issues of cyber crime.[51] This is a team of lawyers that focuses exclusively on issues relating to computer and intellectual property crime. This team operates as the nationally recognised source of advice on cyber law in the USA.[52]

In 1998, The FBI created the National Infrastructure Protection Centre (NIPC). Its mission was to provide a national focal point for gathering information on threats to the infrastructures and providing the principal means of facilitating and co-ordinating the federal government's response to an incident, mitigating attacks, investigating threats and

---

[50] [50] Fighting Cyber Crime: Efforts by Federal Law Enforcement, June, 2001, page 104
[51] http://faculty.ncwc.edu/toconnor/geeelationglory.htm (site visited on 19th June 2006), p.2
[52] [52] Fighting Cyber Crime: Efforts by Federal Law Enforcement, June, 2001, page 104

monitoring reconstitution efforts.[53] According to NIPC, infrastructures are the physical and cyber-based systems that are essential to the minimum operations of the economy and government.

NIPC engages in regular outreach with the industry and ensures there are proper communication channels between the private sector and the government to encourage co-operation on efforts to combat and prevent cyber crimes.[54]

In May 2000, the FBI established the Internet Fraud Complaint Centre (IFCC). Its objective is to identify, track and prosecute new fraudulent schemes on the Internet both nationally and internationally. It has also been tasked with the development of a national strategy for addressing Internet fraud and to refer for prosecution the perpetrators of such frauds.[55]

The USA Patriot Act of 2001 calls for the Director of the Secret Service to take steps to create a network of electronic crime task forces throughout the country based on the model of the New York Electronic Crimes Task Force (NYECTF).

The NYECTF was created in 1995. It focuses on investigating and prosecuting cyber crimes, training and employing computer forensics in their investigations, learning and using the latest technology, researching in and developing new methods of investigating

---

[53] Dick Ronalld L. Cyber Terrorism and Critical Infrastructure Protection, July 2002 www.fbi.gov/congress/congress02/nipc072402.htm
[54] [54] Fighting Cyber Crime: Efforts by Federal Law Enforcement, June, 2001, page 108
[55] ibid p.121

cyber crime. It also keeps in touch with the academia in order to learn the latest trends of cyber criminals.[56]

Computer forensics, which have been employed since 2000, have also enabled cyber attack prevention and the gathering of court admissible chains of evidence using various forensic tools.[57]

These measures of having department and task forces specifically to investigate, prosecute and research on cyber crime help enforce any legislative measures in place. Further, the investing of resources in computer forensics, cyber crime research and detection and the training of those to handle these highly technical crimes, is essential if the war against cyber crime is to be won.

[56] Dick Ronalld L. Cyber Terrorism and Critical Infrastucture Protection, July 2002 www.fbi.gov/congress/congress02/nipc072402.htm

[57] [57] http://faculty.ncwc.edu/toconnor/geeelationglory.htm (site visited on 19th June 2006), p.3

CHAPTER IV

4.0 REASEARCH FINDINGS AND RECOMMENDATIONS

4.1 FINDINGS

4.1.1 Unsolicited Electronic Mail or Spam

The Computer Misuse and Crimes Act 2004 has completely ignored this fast growing problem. The reason advanced by the Chief Parliamentary Legal Counsel in the Ministry of Justice Legislative Drafting Department for this was that it was viewed as a mere inconvenience to the Internet user and in the absence of compelling reasons, did not require criminalising.

Other countries have dealt with the problem of spam differently. While some have opted to criminalise it, others have chosen to handle it as a civil matter. Whatever, the approach, it is evident that the problem of spam is not a mere irritant worth ignoring, but a real threat that requires to be legislated against. It not only threatens individual privacy, but is also an economic burden on Internet Service Providers that have to spend dearly on anti-spamming devices, a cost that is eventually passed on to the unsuspecting Internet user. Thus, rather than just ignore the issue, a more assertive stance should have been taken. It could have either been made a civil offence as is the case in Australia or a criminal one as in South Africa.

4.1.2 Pornography

The Computer Misuse and Crimes Act 2004 has, once again, adopted a non-committal stance to this issue. The reason given by the Chief Parliamentary Legal Counsel in the Ministry of Justice Legislative Drafting Department for this omission was that the stakeholders could not agree on who to target as the offender; should it be the Internet Service Provider (ISP), the end user or the owner of the computer. Thus, it was felt that the provisions in the Penal Code would suffice while trying to sort out this quagmire.

Clearly, different countries have approached the issue of Internet pornography differently. The more liberal Western democracies have focussed more on outlawing child Internet pornography while more conservative countries like India have a provision proscribing Internet pornography in general. For a country like Zambia which has criminalised pornography in general in its Penal Code, it follows that an equally general prohibition should apply to Internet pornography.

The question whether the Penal Code adequately addresses Internet pornography has already been discussed in Chapter II. Suffice to say no provision of the code proscribes accessing or viewing pornography. Thus, if one is flitting from one Website to another neither downloading nor printing anything what offence are they committing? They are neither in possession nor distributing as is required by the Penal Code. In fact, this is the activity the vast majority of users engage in. Not criminalising this act makes the entire Penal Code provisions on pornography a mockery. Who would risk being in possession

of a pornographic DVD when they can watch it on the Internet without committing an offence?

4.1.3 Development and Manufacture for Unlawful Purposes of Devices used in the Commission of Computer Crimes

Despite recommendations in the Computer Society Computer Misuse Bill Discussion Paper (2004), the ensuing Act did not provide for the outlawing of the unlawful development and manufacture of devices used in the commission of computer crimes.

In this global society, such an omission in the Act has the effect of making Zambia a safe haven for the development and manufacture of such devices. This has a negative impact on the entire fight against cyber crime and goes against UN General Assembly resolutions 55/63 of 4th December 2000 and 56/121 of 19th December 2001 which require states to ensure that their laws and practices eliminate safe havens for cyber criminals.

4.1.4 Enforcement Mechanisms

An interview with the Director of Information Technology and Communications in the Zambia Police Service revealed that the police had no unit to deal with cyber crime. What they had instead were three information technology (IT) officers that had undertaken short cyber crime courses in Botswana and France. These officers were expected to train other officers based on the knowledge they had acquired. Cyber crime cases are handled

by the Department of Fraud in consultation with the three cyber crime trained IT officers. Further, assistance can be rendered by Interpol where the crime is of an international nature.

Evidently, the police are ill-prepared to enforce the Computer Misuse and Crimes Act 2004. To leave the enforcement of the Act to two or three officers who have attended short courses on cyber crime is to show a lack of resolve to counter cyber crime.

A further obstacle to combating cyber crime is that the police have not only inadequate expertise, but also inadequate tools to investigate cyber crimes comprehensively. Having provisions in the Act allowing the police to seize all data on a computer suspected to have been used in the commission of a cyber crime without providing the necessary tools and expertise is a mockery.

Of added concern is the fact that little, if anything, has been done to sensitise the citizenry on the existence of this Act. Many asked, including students of law and people working in organisations dealing with computers such as One World Africa and ZAMNET, expressed ignorance of the Act. The failure to publicise this Act so that members of the public are aware of the rights and protection it guarantees them, means many cases of computer related offences go unreported. This too works against the effective implementation of the Act.

4.1.5 Council of Europe Convention on Cybercrime

This is the only authoritative and binding international document on cyber crime. It addresses most issues on cyber crime and obliges state parties to enact legislation in conformity with its provisions. An interview with the Deputy Minister in the Ministry of Foreign Affairs revealed that Zambia has neither acceded to nor ratified this document.

Had this convention been ratified at the time the 2004 Act was passed, issues such as child pornography and the unlawful development of computer devices for the commission of computer crimes would have been criminalised as required by the convention.

The failure to accede to and ratify this convention, again, indicates total lack of resolve by the authorities to deal with the growing problem of cyber crime.

4.2 RECOMMENDATIONS

4.2.1 Unsolicited Electronic Mail or Spam

I am of the view that spam poses a major problem to Internet users. It is through spamming that thousands of pornographic materials can be sent at one go. It is through spamming that numerous frauds through, for instance, advertising non-existent products are perpetrated. In addition, spammers transfer their advertising costs to the unsuspecting

Internet user. This, in my view, is a form of theft which requires criminalising. The question should not be whether it should be criminalised, but how.

The bear minimum should be the approach adopted by the USA, South Africa and Australia which require any person who sends unsolicited commercial communications to provide consumers with the source of the email as well as an opportunity to opt-out from receiving further emails from that source. Failure of anyone to do this should attract criminal sanctions. This should be a fine or prison sentence depending on the extent of damage done.

4.2.2 Pornography

Clearly a separate provision outlawing Internet pornography is required. This should be extended to accessing so that anyone who knowingly and intentionally views pornography on the Internet is guilty of an offence.

Due to the mammoth task involved in policing whether or not individual users are accessing Internet pornography, the law must provide for ISPs to take reasonable steps to curtail the distribution and accessing of pornography. Being the first point of entry of these materials and having the technical know how to do so, they are better placed to control the entry and transmission of these materials. The failure by an ISP to take reasonable steps to do this must carry a sanction, preferably a fine.

Thus, in my opinion, both the end computer user and ISP must be targeted with regard to Internet pornography if Zambia still maintains the stance that pornography is an offence.

4.2.3 Development and Manufacture for Unlawful Purposes of Devices used in the Commission of Computer Crimes

There is need for the Act to have a provision proscribing the unlawful development and manufacture of devices used in the commission of cyber crimes. This is in line with Article 6(1) of the Council of Europe Convention on Cybercrime which commits state parties to criminalise not only the distribution, but also the production of devices used in the commission of computer crimes.

4.2.4 Enforcement Mechanisms

There is need for the Act to provide for the establishment of a unit within the Police Service dedicated to cyber crime. This will ensure a competent body of experts within the force to deal with the crime. It will also enable the force keep abreast of the ever evolving crimes in this sphere.

In the interim, in the training of police offices and lawyers, the criminal law component should include cyber crime. Eventually, cyber crime should be introduced as a separate course in legal training. Training institutions, particularly for the police, should be well equipped with fully fledged computer laboratories for this purpose.

Judges and magistrates, who play a vital role in interpreting the law, also need to be well versed in cyber crime. Therefore, they must be equally trained in this regard. Further, due to the dynamic nature of cyber crimes, they must be more liberal in their interpretation of cyber crime provisions. Thus, provisions should be liberally interpreted so that a crime that may not have been envisioned when the Act was being enacted can be catered for.

Finally, there is need for the police, in conjunction with other stakeholders such as the Banker's Association of Zambia and the Computer Society of Zambia, to raise awareness of the Act among citizens. This is to prevent cases of computer crimes going unreported due to lack of knowledge.

4.2.5 Council of Europe Convention on Cybercrime

There is urgent need for the Government to accede to and ratify the Council of Europe Convention on Cybercrime, the only international agreement on the subject, if the issue of cyber-crime is to be treated with the seriousness it deserves.

CHAPTER V

5.0 CONCLUSION

In Chapter I, the study identifies cybercrime as a growing worldwide concern with repercussions on the economic and social wellbeing of society. It goes on to show how the rampant bank frauds and hacking of State House Website galvanised Zambia into enacting the Computer Misuse and Crimes Act in 2004. It further shows that because the legislation was reactive rather than proactive, focus was on computer fraud and access to protected sites. Thus, issues such as Internet pornography, unlawful manufacture of devices used in the commission of computer crimes, spam and enforcement mechanisms were not catered for.

Chapter II analyses the shortcomings of the Act. These include its failure to address Internet pornography, the growing problem of spam, unlawful manufacture of devices used in the commission of computer crimes and enforcement mechanisms.

Chapter III gives an international perspective of attempts to deal with cyber crime. It looks at the measures the United Nations, G-8 countries, Commonwealth and Council of Europe have taken to combat cyber crime with the most important being the adoption of the Council of Europe Convention on Cybercrime. It then looks at how some states have legislated on the issues identified in Chapter II as the shortcomings of the Computer Misuse and Crimes Act 2004. For instance, it shows how spam has been treated as a civil

matter by some states and a criminal one by others. It also shows how the general consensus is that, at the very least, computer crime legislation should proscribe child pornography. Further, it shows how some states such as the United States of America have established departments such as the Computer Crime and Intellectual Property Section to look specifically into issues of cyber crime.

Chapter IV has shown that rather than deal with the issues of spam and pornography, the Computer Misuse and Crimes Act 2004 has chosen to ignore them. The former was ignored because it was perceived as a mere irritant rather than a problem while the latter was ignored because of failure to determine who to target. This chapter has gone on to make several recommendations. To begin with, it recommends that spam should be criminalised. It further recommends that the possession, distribution and accessing of Internet pornography should also be criminalised. In addition, Internet Service Providers should take reasonable steps to curtail the transmission of Internet pornography. The failure of an ISP to do this should attract sanctions. Another recommendation is that the development of devices used in the commission of computer crimes should be outlawed. To enhance the enforcement of the Act, it has been recommended that a well equipped cyber crimes department be established in the Police Service. Further, legal training for both lawyers and law enforcement officers should include a component of cyber crime. Finally, Zambia should accede to and ratify the Council of Europe Convention on Cybercrime.

From the foregoing, it is evident that while Zambia has attempted to combat cyber crime through the enactment of the Computer Misuse and Crimes Act 2004, there are a number of issues of concern that this Act has failed to address. It is, therefore, incumbent upon the Legislature to review the Act in order to cater for these issues. Other ancillary measures such as the ratification of the Council of Europe Convention on Cyber Crime and establishment of a unit in the Police Service to deal specifically with issues of cyber crime should also be put in place. Failure to do this will make this piece of legislation, like many other laws in our Statute books, impotent.

BIBLIOGRAPHY

ARTICLES/PAPERS

Archaic Laws Threaten Global Information, December 2000

Bankers' Association Correspondence to the Ministry of Communications and Transport, 4th June 2002

Child Pornography: Model Legislation and Global Overview, International Centre for Missing and Exploited Children, 2006

Computer Related Criminality: Analysis of Legal Politics in the OECD (1986)

Ronalld, D. L. *Cyber Terrorism and Critical Infrastructure Protection*, July 2002

Fighting Cyber Crime: Efforts by Federal Law Enforcement, June, 2001

Goldman, E. *Where's theBee? Dissecting Spam's Purported Harms*, 2004

Harmonising National Legal Approaches on Cybercrime, International Telecommunications Union, 2005

Report on Computer Misuse Legislation, Zambia Law Development Commission, 1998

Schjolberg, S and Hubbard, A. M. *Harmonising National Legal Approaches on Cybercrime*

Steyn, T. *Zambia to Fight Cyber Crime*

BOOKS

Lloyd, Ian J. Information Technology Law Fourth Edition, Oxford University Press, Oxford, 2004

Bone, S (Ed) Osborn's Concise Law Dictionary Ninth Edition, Sweet & Maxwell, London, 2001

Yaman, A.*Governance of Pornography and Child Pornography on the Global Internet: A Multilayered Approach*, Edwards L and Waelde C. eds, Law and the Internet: Regulating Cyberspace Hart Publishing, 1997

CONVENTIONS

Council of Europe Convention on Cybercrime

JOURNALS

Alongi, E. A. Has the US Canned Spam? Arizona Law Review Volume 46, 2004

Sorkin, D. E. Technical and Legal Approaches to Unsolicited Electronic Mail, University of San Francisco Law Review Volume 35 2001

Speer, D. L. Redefining Borders: The Challenge of Cyber Crime Crime Law and Social Change Volume 34 2000

STATUTES

AUSTRALIA

Spam Act 2003

INDIA

Information Technology Act 2000

SOUTH AFRICA

Electronic Communications and Transactions Act, 2002

UNITED KINGDOM

Child Pornography Act 1978

Criminal Justice and Public Order Act 1994

Obscene Publications Act 1959

Protection of Children Act 1978

UNITED STATES OF AMERICA

CAN SPAM Act 2003 117 STAT

ZAMBIA

The Computer Misuse and Crimes Act No. 13 of 2004

The Penal Code Act Cap. 87 of the Laws of Zambia

WEBSITES

http://cincsa.info/portal

http://faculty.ncwc.edu/toconnor/geeelationglory.htm (site visited on 19th June 2006)

http://vjolt.student.virginia.edu/graphics/vol4/home_art4.html (site visited 18/07/06)

www.fbi.gov/congress/congress02/nipc072402.htm

www.mcconnellinternational.com

www.cse.stanford.edu/class/cs201/projects98-99/computercrime (site visited 09/06/06)

www.dataprotection 2003.info/Speakers/Maijan (site visited 09/06/06)

http://www.naavi.org/pati/pati_cybercrimes_dec03htm (site visited on 16-10-06)