NAMIBIAN ECT BILL & COMPUTER BREACHES

W.S. Kaniita

Masters of Information Technology

2008

MASTER'S MINI-THESES TITLE: NAMIBIAN ECT BILL & COMPUTER BREACHES

Author' Name: Werner Simaneka Kaniita

"Thesis/Mini-thesis presented in partial fulfilment of the requirements for the degree of Masters of INFORMATION TECHNOLOGY at the Polytechnic of Namibia

First Supervisor: Prof Dr. David E Cook (Polytechnic of Namibia)

Second Supervisor: Dr. Paul Ludik (external)

Date and Year: June 2008

Declaration

I, **Werner Simaneka Kaniita**, hereby declare that the work contained in the mini–thesis, title **Namibian ECT Bill and Computer Breaches**, is my own original work and that I have not previously submitted it, in its entirety or in partially at any institution for the award of a degree.

Signature:…….. Date:……..

Retention and Use of Mini-Thesis

I **Werner S. Kaniita** being a candidate for the degree of Masters of **Information Technology** accept the requirements of the Polytechnic relating to the retention and use of Master's Thesis /Mini-Thesis deposited in the Library.

In terms of these conditions, I agree that the original of my thesis/mini-thesis deposited in the Library will be accessible for purpose of study and research, in accordance with the normal condition established by the Librarian for the care, loan or reproduction of theses/mini-theses.

Signature.....Date:.....

Acknowledgements

My gratitude goes to my two supervisors: Dr. P Ludik, The Director of the National Forensic Science Institute, in the Ministry of Home Affairs, in the Republic of Namibia and Prof. David Cook at the Polytechnic of Namibia. Without the supervision of these two professionals, this thesis would not have become a reality.

I would also like to thank my wife Paulina N. Kaniita and my twin daughters, Landuleni & Landula and not to forget my last born boy Mbwangu, for humble time that I was away from them. I left home at 6h45 almost every single day and only to return back home at around 22h00. They have always missed me, when I was away busy on my research. Thanks for your understanding when I was away from home, without giving you the love and the attention you deserve.

In addition the author acknowledges the contribution of the following people: Professor Susan Brenner, fellow student Panduleni Edi-Oshili Ndilula and fellow Masters Candidates at the Polytechnic of Namibia, for the support rendered during this research.

Last, but not least I want to dedicate this work to my late father Shikongo Simon Kaniita, who contributed so much to what and where I am today.

Abstract

This mini-thesis examines the impact and effectiveness of the Namibian ECT Bill, which is still to be passed in the Namibian parliament. The Namibia ECT Bill in its current format, will it be effective in an attempt to combat cybercrimes and computer breaches? Internet has taken over and plays a role in everybody's daily lives. People are connected to the internet from everywhere. They connect to cyberspace where there is access to the internet i.e. at their home, at their office, at the restaurant, at the airport, etc. Subsequently, people are conducting business online, forming online contracts via the internet. In other words e-commerce is a reality because of the information highway and internet.

This mini-thesis has looked at the cyber crime cases that some countries have experienced where the law enforcement agency was seen to be useless or powerless. This was due inadequate cyber law or the cyber activities were not a crime at that point in time, in that particular country. Despite damages and losses suffered as a result of such cyber activities, suspect(s) remain free and never faced the law.

Contractual issues over the internet have been explored during this research. There are questions that; for example, when the contract is concluded, what are the terms of contract and how the law is going be applied to the online contract.

The mini-thesis examined concerns about the electronic signature and the Certification Authority. The provision for electronic signature in the Namibian ECT Bill has been compared against similar acts in countries that have similar legislation in place. Other issues of concern are that each country has defined its ECT Act differently from other countries. This differences have led to a situation where what is legal in one country, is illegal in another country.

The mini-thesis has also looked at issues of cyberspace jurisdiction. Many references have been highlighted as to what might be the possible solution to cyberspace jurisdiction.

Some comparisons are highlighted in this mini-thesis, with an attempt to show the similarity and differences between the Namibian ECT Bill and other countries' ECT Acts.

A few cybercrime cases have been covered in this mini-thesis. Some of the suspects appeared before the courts but could not be successfully prosecuted therefore, ending in acquit.

Table of Content

CHAPTER 1: INTRODUCTION

1.1 Introduction

1.1.1 Background

It is fact that the use of Electronic Commerce Transactions (ECT) and Electronic Data Interchange (EDI) are becoming more a part of our daily life. This is due to information and communication technologies development. Chawki (2005) stated that "The introduction, growth, and utilisation of information and communication technologies have been accompanied by an increase in criminal activities"

Ahsan (2007) explained that "Moreover, as computer and the internet technologies advance, criminals are using cyberspace to commit various types of cyber-crimes under the disguise of ordinary online transactions and communications".

Information and Communication Technology (ICT) has make life easier for most of people in the world. People are even becoming lazy because of the use of the Internet. Internet is now offers anything that you can imagine i.e. from fully internet banking to e-commerce. These transactions are conducted over the internet, in cyberspace, which has no physical boundary limitation. It is also a known fact that people can conduct transactions between different countries and different continents as well.

As Internet users enjoy the benefits of Internet, there are possibilities that cybercrimes and illegal activities are committed over the internet. This necessitates some states to develop new legislation on cyber matters. Kondo (2002) pointed out that "Internet law, like any other complex high technology cases, constantly challenges the competence limits of the legal system."

Hong (1998) stated that there is a change on how people have used the internet. Hong further said that: "Initially, researchers and educators used the Internet for the free exchange of information. The Internet rapidly grew in popularity and currently has twenty-five to forty million users. Today, most Internet users access it for mainstream commercial purposes. As the Internet expands, however, so does a new type of crime -- computer crime".

Electronic and communication transactions may take place between two parties from everywhere in the world. Dispute(s) may arise out these electronic transactions. In case of a dispute arise, which country's law will be applicable to such dispute? Each country has its cybercrime law defined different from that of other country, base on it physical boundary while there is no physical boundary limitation in the cyberspace.

Swanson (2002) stated that "the law governing E-Commerce, Information Technology and the Internet is rapidly changing and it is impossible to be current on any issue for long."

The existing cyber laws and other domestic laws are outdated or inadequate to address and regulate issues and activities in cyber space. Watney (2007b) pointed out that "the electronic medium challenges the designed for a physical medium." Online transactions are done and conducted electronically, on the cyberspace. Cyberspace knows no physical limitation in terms of our physical border and boundaries.

Parties may enter into trade contracts or any other agreement by means of electronic communications. Kondo (2000) further pointed out that "The internet is unique in that it permits parties in remote locations to instantaneously, at the click of the mouse, enter into a contractual agreement with performance independent of the parties' physical sites or the information involved".

It is possible for cyber criminals to commit criminal activities over the internet from anywhere in the world. A cybercriminal may commit that crime in Namibia, without the cyber criminal being present in Namibia. Is the Namibian ECT Bill formulated to deal with such internet crimes or any other unethical activities over cyberspace?

1.1.2 Problem Description

The Internet and cyberspace is here to stay. This mini-thesis will highlight the similarity and the differences, which might be found in the Namibian ECT Bill in comparison with similar acts. The question is that, is the Namibian ECT Bill formulated in such a way that it will be effective, once enacted, to deal with all the cybercrimes and computer breaches? What activities in the cyberspace are going to be outlawed and criminalized in Namibian context? What is not criminalized in the Namibian ECT Bill and what will be the impact of such exclusion?

Interestingly, cybercrimes and computer breaches may be committed in a jurisdiction without the perpetrator(s) being physically present in that same jurisdiction. How will the Namibian ECT Bill deal with such issues around jurisdiction? Another issue is how the Namibian ECT Bill will deal with extradition of criminals and also with the jurisdiction disputes emanating from cybercrimes? Will Namibia be in a position to claim jurisdiction on perpetrator(s) residing somewhere else i.e. in another jurisdiction?

Some countries have amended their existing laws and legislations to enable them to better deal with cybercrimes and computer breaches. According to the report by McConnell International LLC (2000) and I am quoting, it was stated that: "Such countries have also enacted such laws and legislation to boost international cooperation and investigation"

Watney (2007a) stated that "Little did countries realize that the increasing use of computers would result in growing dependence on computer systems for the daily functioning of the countries' various services and that such services may expose the country to certain vulnerabilities such as possible attacks launched against the systems."

Nowadays the world has become a global village due to development and advancement of information and communication technologies. Grabosky (2000a) has stated that "It is trite to describe the ways in which computers have, figuratively speaking, made the world a smaller place. The corresponding potential for trans-jurisdictional offending will pose formidable challenges to law enforcement. For some crimes, this will necessitate a search for alternative solutions."

The global village concept is because of information and communication technology development. Students doing their study research might not necessarily need to meet them face to face with their supervisor they may do online. Students can be supervised by any professor from anywhere in the world. This is made possible by the use of the internet and information highway.

States and countries, Namibia included, need to take different approaches on the issues of dealing with cybercrime and computer breaches. Countries have to strategise on how to deal with the challenges faced by the law enforcement agencies. Jurisdiction is one of the main issues that are still unresolved. Another issue is the existing domestic law versus the Convention on Cybercrime and the Model Law, where the recommendation on the Convention will violate the existing law. The challenge is on how to merge the two i.e. the existing domestic law not to be in contrast with the Convention and the Model Law.

According the Namibian E-laws Working group, the overall objective of the Namibian ECT Bill is "to enable, facilitate and promote the use

electronic communications and transaction conducted via electronic communications and generally, with various forms of information. The ECT bill aims to encourage the use of ICTs and e-government and e-commerce services and furthermore to protect the public, consumer and clients from misuse and unauthorised use of the ICTs, and to provide penalties for misuse."

Referring to cybercrime and South Africa' ECT Act No. 25 of 2002, Herselman and Warren (2003) stated that "Research needs to be done on how badly South African companies are affected by cyber crime (if at all) and whether the newly promulgated laws will aid in preventing and prosecuting these crimes."

Ahsan (2007) has explained that "The best way to promote domestic defence is to dramatically improve the capabilities of law enforcement and other agencies that look after our safety and well-being every day".

The European Convention on Cybercrime and the UNCITRAL Model Law are some of the relevant steps taken to guide any state to formulate its cyber law, which may be used to resolve and reduce challenges faced by law enforcement authority with respect to cybercrimes and computer breaches. Any country may sign the Convention by invitation of a member state. Thereafter it may adopt and become signatory to the Convention on Cybercrime. When the Convention is signed by a state, it may become part of that state's law or that state may adopt some parts of the Convention.

The main goal of the Convention as summarised by Archick (2004), "is to establish a "common criminal policy" to better combat computer-related crimes worldwide through harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation".

There is nothing in the Convention, forcing any state to implement the Convention on Cybercrime in fully; it all depends on the state, on how that state has taken the Convention into consideration. "But in practise the Convention features a set of exceptions to mutual assistance. Nations may refuse to cooperate with request that involve a "political offence "or if a country believes the request would prejudice its sovereignty security, public order or other essential interests" (Arnold, 2007a).

The concept of the "common criminal policy" will be a success and achievable, if all states in the whole world speak one language in terms of cybercrimes and computer breaches. Currently a state may apply some of the provisions in the Convention or whole of part of it. This will leave some loopholes in the whole effort to combat and prevent cybercrimes and computer breaches. In some states, i.e. United State of America, freedom of expression is guaranteed, while in other country i.e. France, it is not the case. In the USA, as a result, the Convention on Cybercrime not ratified as a whole.

Mills (2003) pointed out that "In December of 2001, the United Nations Commission on International Trade Law ("UNCITRAL"), issued, by Resolution of the General Assembly, a Model Law on Electronic Signatures (the "MLESig"), offered to any and all states that may wish to adopt it, and intended to be adopted together with UNCITRAL's Model Law on Electronic Commerce (the "Model Law")". It is my opinion that the Namibian ECT Bill has been drafted with input or in line with the Model law.

This mini-thesis will consider the cybercrime cases from the courts in some other states. Further, the mini-thesis research will:

a) Consider papers and publication on internet about cybercrimes and computer breaches.
b) Consider expert opinion to compare with our Namibian ECT Bill.

c) Benchmark the Namibian ECT Bill with the recently updated cyber laws, taking into considerations what have so far come before court and what problem encountered in applying such cyber law.
d) Listing all the possible cybercrimes and computer breaches to see if they are taken care in the Namibian ECT Bill.

The Namibian ECT Bill needs to make provision for extradition, for any commission of cybercrimes and computer breaches. Cybercrimes might be committed from beyond the Namibian border, but have effect in Namibia. It will not be unique for Namibia, to face challenges in implementing its court decision on foreign jurisdiction as far as cybercrime cases. This has been experienced, by other states like France and Philippines.

As it was stated before disputes may arise out of these electronic transactions, between the parties to any contract. The disputes as such, may results into litigation. There will be no problem, in trying to resolve these disputes, if all the parties to the dispute reside in one jurisdiction i.e. same country. They both will be subjected to that country's relevant and applicable law. If these two parties reside in different countries, then it will be an issue. The question will be as to which country's law and legislation, such dispute to be subjected to?

The answer to the question above depends upon cooperation between states. Magnin (2001) said that "As computer crimes are often international in their nature, national measures need to be supplemented by international cooperation."

1.2 Conclusion

Internet knows no boundary limitation as Mills (2003), states that "because of borderless nature of electronic commerce, the same can

be regulated smoothly, safely and consistently on an international scale, only if there is a single universal framework, within which all legal systems will operate."

The idea of universal framework will be made possible with the help of the Convention on Cybercrime. But countries that did not participated in its formulation are not allowed to freely join the Convention. The Convention on Cybercrime will improve the combating and fighting of cybercrimes by making cyber crimes as extraditable offences. If all countries became parts of the Convention, this will leave little room for cybercriminal(s) to hide. They will not be able avoid prosecution any more once all countries in the world has single universal framework.

It is also notable that the Namibian ECT BILL has so far defined the jurisdiction on a par with most recent legislation development. When cyber crimes are committed and have effect on Namibia that will give, a Namibian court, a jurisdiction to adjudicate on such crimes. Even if such cybercrimes were committed externally, Namibia will have jurisdiction over such cyber crime, according to provisions in the Namibian ECT Bill. This provision is more or less, similar to some ECT acts like that of Mauritius (THE COMPUTER MISUSE AND CYBERCRIME ACT 2003, Act 22 of 2003) and Singapore (COMPUTER MISUSE ACT (OF SINGAPORE)). With such a provision in the Namibian ECT Bill, Namibia will avoid the situation that was faced by FBI in the "Love Bug" virus saga. The Love Bug suspect cannot be extradited or even arrested due to lack of relevant law or inadequate law in that specific country.

Angelopoulou et al (2007) concluded that "as ID fraudster have discovered new tools, so must forensic investigators and Law practitioners in order to be able to cope with the trend and tackle it effectively."

Damage done in Namibia, as a result of cyber crime might be damage in South Africa and everywhere. Love Bug caused damage worldwide.

As a result most companies and organisations were affected negatively in of financially terms. Watney (2007b) pointed out that **"**the release of the "I love you" virus in 2000 caused substantial global economic loss. The suspect was traced back to the Philippines, but this action was not criminalized in the Philippines at that stage**."**

There should be no place to hide for someone who had committed a cybercrime or a computer breaches. Countries should adopt a common ground when they outlaw cyber activities, so that similarly crimes are outlawed everywhere, in any country.

1.3 Structure of the Mini-Thesis

Chapter One

This chapter presents the description of this mini-thesis. It discusses cybercrimes that pose difficulties to law enforcement agencies. This chapter explains the background of the report on cybercrime and computer breaches. The chapter goes further in details of the problem description and it also highlights the possible solution to the problem highlighted in the problem description part of this thesis.

Chapter Two

This chapter deals with the legal aspects concerning cyberspace. Notable examples of cases that come before court of law are highlighted in this chapter. The chapter further describe how the court where facing difficult on dealing with such cases.

Chapter Three

This chapter describes contracts that can be concluded online. It touches on the question raised concerning the online contract formation, and also when such contract can be accepted. The chapter also looked at legal recognition of the data message and the online contract formation.

Chapter Four

This chapter is concerned with the electronic signature in comparison to provisions made in the Namibian ECT Bill with similar provisions in the similar cyber laws from other countries.

Chapter Five

This chapter discusses and compares the Namibian ECT Bill with other legislation that has been enacted. It highlights the differences on how each country had outlawed and criminalized some actions in the cyberspace.

The chapter further suggests a single universal frame work that can be formed by the countries connected to the internet. The chapter concludes by recommending some actions that needs to be taken so that there is similarity in each country's cyber law.

Chapter Six

This chapter deals with conflicts and very interesting cases about jurisdiction in the cyber space. It highlights the different approaches to cyberspace jurisdiction. It refers to the Convention on Cyber crime which tries to resolve the issues of cybercrime and serve a guide to the formation of ECT acts.

The chapter further presents the possible conflict in cyberspace jurisdiction and possible solutions to such problems.

Chapter Seven

This chapter deals with the tax implications for the e-commerce. The concern in this regards is whether the existing tax law will be applicable to the commercial activities in cyberspace.

The chapter also highlights some possible fraud in connection with the e-filing of income tax returns that was experienced by the Internal Revenue Service (IRS, American tax authority).

Chapter Eight

This chapter deals with cybercrime cases that have so far come before the courts. It highlights the main focus about how it was difficult for the court to deal with the case before it due to inadequate law or due to domestic law.

The chapter raises some questions as to why the cyber laws are defined differently from country to country.

Chapter Nine

This chapter deal with the methodology used during the development of the mini-thesis. This chapter presents the data collection method and some other problem encountered during this research.

Chapter Ten

Chapter Ten presents the recommendation, the conclusion and also further recommendation for study in this field.

CHAPTER 2: CYBERSPACE LEGAL FRAME WORK

2.1 Introduction

What are we referring to when we talk about cybercrimes and computer breaches? How is it defined by states or government or by law enforcement agencies?

Arnold (2007a) pointed out "that some theorists have argued that we now live in a borderless world where people, capital, information permeate through jurisdictional boundaries at will."

So far researches have shown that cyber crimes may be committed from one country and also that cyber crimes might have effect and cause damage in several countries. This has created a dispute as to which country's law is applicable to such cyber crime and which country may claim jurisdiction because that cyber crimes involves many countries

There are some definitions of cybercrime on the internet. Babu (2004) defines cybercrimes as: "It is a criminal activity committed on the internet. This is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money".

These days cybercrime should be a concern to each law enforcement agency. Interpol has also listed cybercrime among its top five priority crime areas, as it came seen below.

Fig 1 : Five priority crime areas of INTERPOL
SOURCE: http://www.interpol.int/

Cybercrime is not defined in the Namibian ECT Bill. There is also no definition of the term cybercrime in the Convention on Cybercrime. This might be of no great importance on how we define the term cybercrime.

Cybercrime is not a new phenomena or a new crime as such. It is rather another "modus operandi" on how the specific crime was committed due to information and communication technologies advances. It is important to have a legal frame work that counters or combats whatever illegal activities that are conducted in the cyberspace.

Another definition of cybercrime, according to Goodman and Brenner (2002a) is as follow: "the terms "cybercrime," "computer crime", "Information Technology crime," and "high-tech crime" are often used inter-changeably to refer to two major categories of offences: 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 offences -- 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"

Kende (1997) commented that "although most individuals who use the Internet do so through a computer, many may soon use their television sets to access the Internet." This is where and how information and communication technology will be advanced in the future.

The mode of operation on how the criminal activities were conducted and carried out is what makes the criminal activities to be referred to as cybercrime. As stated before neither in the Namibian ECT Bill nor in the European Convention on Cybercrime (here in referred to as The Convention) is the term cybercrime defined. I think it not necessary to define the term in the act.

2.2 CYBERCRIMES IN THE NAMIBIAN ECT BILL

There are types of cybercrimes listed in the Namibian ECT Bill. Those listed are more or less the same to the cybercrimes that is in the European Convention on Cybercrime. Namibia did not participate in the drafting of Convention on Cybercrime and Namibia is also not a signatory to the Convention. But it is commendable move, by the Office of the Prime Minister in the Namibian government the way the ECT Bill is defined. Most of the provisions are in line, with the recommendation of the Convention. Recent developments, be it on an international level or regional level, were considered in the drafting the ECT Bill.

It seems of no importance on defining the term cybercrime. Grabosky (2000b) stated that "The variety of criminal activity which can be committed with or against information systems is surprisingly diverse. Some of these are not really new in substance; only the medium is new."

The Namibian ECT Bill seeks to make statutory provision for cybercrimes and computer breaches as part of the existing Namibian law. Even thoughts crimes might be defined in another existing Namibian criminal law other than the Namibian ECT Bill, the ECT Bill has make provision, listed and defined the criminal activities. The offences provided for, in the Namibian ECT Bill, are in relation to:

- Attempting and aiding and abetting;
- Unauthorised access;
- Unauthorised interception;
- Unauthorised interference with data or information systems;
- Misuse of services;
- Electronic fraud or forgery, and
- Electronic extortion

Countries like Singapore, Malta, Sri Lanka, Northern Territory of Australia, just to mention but a few have criminalised the same offences in their cyber laws similar to the provisions in the Namibian ECT Bill. There might be slight differences in the order of the wording or the clauses, but the aims and the objectives are the same in terms combating of cyber crimes and computer breaches.

2.3 CONSEQUENCES OF INADEQUATE LAW

Some countries were faced with difficulties when dealing with cybercrimes cases. This was due inadequate cyber laws or legislations at the times the cybercrime was committed. These countries are the Philippines, France, Norway and the USA.

Three good examples of cyber crime cases that were encountered have been selected for the purpose of this mini-thesis. These cases should be good and sufficient reasons as to why each state needs to redress and update their cyber laws and legislation dealing with cybercrime and computer breaches.

2.3.1 DVD CASE

This case is about the Norwegian boy, Johansen well known as DVD Jon. He created a program to decode the code that prevents the copying of DVD. Johansen makes the code available for use by anyone, on the internet.

Johansen was taken to court but due to the inadequate law governing the alleged offences in question; Johansen was acquitted of all charges. Kolsrud (2003) stated that "The court ruled there was "no evidence" that either Johansen or others had used the decryption code (called DeCSS) for illegal purposes. Johansen therefore couldn't be convicted on such grounds, nor for acting as an accessory to other alleged illegal activity, wrote judge Irene Sogn in the court's ruling."

Chief prosecutor Inger Marie Sunde now says the Norwegian government's case against Mr. Johansen was hindered by an ambiguous law and the difficulty in proving "the connection between something that you have posted on the Internet and the damage done by it.

For his role in writing DeCSS, Johansen was charged with breaking the Norwegian law that prohibits gaining unauthorised access to data, and then was acquitted twice when the court ruled that the data were his own (Levine 2006).

Realising that its cyber law is not adequate, the Norwegian government took a necessary step to amend it laws. Stecklow (2005) stated that "in June 2005, Norway overhauled its copyright law, making illegal the posting of a program that defeats a DVD's anti-copy protection technology."

The overhaul comes in only after the damage had already been done. Unfortunately the Norwegian copyright law cannot be applied retrospectively. Other states should learn from this.

2.3.2 Love Bug case

The love bug case is a well known case in the cyberspace world. In this case, there was a virus which spread over the cyberspace, causing damage worldwide. The virus was traced back to be originated and created in the Philippines. At the time this happened, there was no law that prevented anybody from making or creating a virus in the Philippines (Brenner & Koop, 2004).

The Philippines' law agency could not do anything in terms of arresting a suspect. The whole processes of arresting the suspect and the court proceeding was delayed as a result of inadequate laws. "Bringing to book a perpetrator who operates on an international scale in the distribution and or hosting of child pornography for the commission of cybercrime is easier said than done" (Watney 2005).

Subsequently the Philippine state did enact the relevant law in connection with creation and dissemination of worms or viruses. The Philippines government only update the cyber law and outlaw the distributions of viruses, after the damage had already been suffered.

2.3.3 The Nazi Auction case

This case is about the Yahoo! Auction case, an USA corporation, which sells Nazi items online on its website. The items were on sale in USA online, which are accessible and viewable online in France, ***Hayashi (2005).*** In France it is illegal to display the Nazi items online and in public. This resulted in a court case being launched in France against Yahoo! Inc., a USA corporation.

The French court ordered Yahoo! Inc. to eliminate the French citizens' access to any Nazi materials available online. However the French court could not impose or enforce its jurisdiction decision on the Yahoo! Corporation as it was located in USA, which is another jurisdiction. USA was not obliged at all, to implement the decision by the French court. The court in France could not do anything to enforce its decisions in USA. According to USA law such a company has done nothing wrong within its jurisdiction.

The situation above can be faced between any countries in so far as their law and legislation differ for the illegal activities.

Reidenberg (2005) stated that "The recognition of foreign judgements in these attack cases will often be problematic. As the Yahoo! illustrated, public order rules at the place where internet activity is launched may conflict with those of the place where the activity has its effect."

In USA, it is not an issue and it is legal to make the Nazi items available online, as the freedom of expression is guaranteed by the Fourth Amendment. Whilst in France, the Nazi items are regarded as causing injuries to national interests, such as unrest to public order; therefore it is illegal to make such items available online.

2.4 CONCLUSION

Illegal activities over the internet should be made punishable offences, in all laws of nations. The Namibian ECT Bill is in line with current developments; be it on the regional or international level, in outlawing criminal activities over the cyberspace. The cybercrimes and computer breaches provided for in the Namibian ECT Bill are similar to most of the countries in the world.

In the Namibian context, the access without authorization is illegal and it is a punishable offense, when the ECT Bill becomes an act of

parliament. Namibia goes further making it punishable offense for unauthorised interference and interception to any data or information systems.

Any possible illegal activities online should be criminalized under the Namibian laws, to avoid reactions only after the damage had already been done. "*It is evident that internet usage requires laws and regulatory authorities, which should span across national boundaries and legal systems* (Jahakhani, 2007).

Cooperation among the states is needed when it comes to activities that are criminalised in one country and the activities not criminalised in another.

CHAPTER 3: CONTRACT OVER THE INTERNET

3.1 Introduction

It is possible today to conclude a contract online due to the use of the internet. Christensen (2001) defines a contract as "the primary mechanism for the transaction of business. A contract may be described as an agreement under which parties assume obligations to each other for valuable consideration".

The Namibian ECT Bill's aim is to provide the public with legal certainty and trust in everyday electronic transactions in all spheres of internet activity. The Namibian ECT Bill is promoting the use of e-commerce, the use of conducting business online and many other use electronic transactions for businesses purposes or to make life easier for the Namibian's inhabitants.

Argy and Martins (2001) highlighted that "there is a shift towards electronic contracts, which are now being executed by email or over the internet between parties with no previous relationship". They asserted that the enormous growth of the internet as a facility for effecting electronic transactions has introduced concerns and challenges for businesses, consumers and lawyers alike.

The Namibian ECT Bill, once enacted, will make provision for the public to conduct business online. This means the public may form and conclude contract online without them being in the presence of one another. Such contract will be valid and legal within the Namibian law.

3.1.1 When, What, How, etc.

However it seems that there are still issues about online contract. Mills (2003) raised some questions that "how does one determine or, more importantly, prove WHEN an agreement has been reached and WHAT are the terms of that agreement? What law will apply to that agreement, and what governing body has jurisdiction over that agreement and/or the parties thereto?"

Furthermore Arnold (2007a) said that "there are questions about where online activities take place. There are questions about the location or nature of any dispute resolution mechanism, since few regions have identical laws".

Most of these questions are addressed in the Namibian ECT bill on provision that the data message may be used in forming the online contract. The provision further prides that the contract should not be denied any legal recognition just because the formation of such contract was done by means of data message.

When the ECT Bill becomes an act, a contract formed and completed online, will be a valid and legal contract within Namibia physical boundary. What will happen in the case that one want to form or enter into a contract with a person from elsewhere, in the world, where there is no such cyber law or similar law in place?

The same question was also asked by Hamano (2000) that **"**if a contract between persons residing in different countries was made entirely on the Internet, which country's law apply?" The answer to this question will lie on the cooperation between those countries, provided that their relevant law are defined in the same way. This seems still the issue that when the dispute arose between the parties to contract from different countries. I believe no country can solve this alone without the cooperation of another countries.

3.2 Contract Formation by Electronic Means

Contract may be formed electronically or entered into electronically, between the parties by means of e-mail exchange, by filling and submitting the forms on line, pressing or clicking the "submit" button. This can be done without the parties to the contract, knowing each other before and without having seen one another.

It not clear as to which jurisdiction's cyber law will be applicable to such online contract, in case of a dispute arising between the two parties to the contract formed by electronic means over the cyberspace.

The point raised by (Argy and Martins (2001)) is actual true, especially when it comes to the dispute between parties from different continents. People may, by means of online and by way of email start to communicate and do business. There after enter into a buying/business contract. A problem will start when the other party fail to deliver things/products/services as agreed in the contract. The possibilities exist, that the other party to such contract might act outside the contract parameters.

The Namibian ECT Bill is silent about some of the questions raised above. If the contract is formed by electronic means within the Namibian boundary, it will be no problem, as it will be a valid contract. What about if the contract formed between the parties, one party resides in Namibia and the other party is located elsewhere in the world? One might say it is covered under jurisdiction in the Namibian ECT Bill. Will extradition, jurisdiction enforcement, be possible under the proposed Namibian ECT Bill? The Namibian ECT Bill is silent about such topics. It might be that such issues are dealt with by other existing laws. This problem is not specific to Namibia a country alone, but to all nations/states in the cyber space.

3.3 Acceptance of an Online Contract/Offer

The Namibian ECT Bill makes a provision as to when the offer and the data message become effective or when the offer deems to be accepted. This provision is different from other ECT acts, e.g. the US, UCITA. Section 215 of UCITA have the following section for the effective and effect of acknowledgement, which seem to be differently from others, but very interesting in terms of how the data message will be received, i.e. "(a) Receipt of an electronic message is effective when received even if no individual is aware of its receipt."

Other cyber laws make a provision that the acceptance of the offer is effective upon such data message being accessible to the addressee. Like in the case of Malta's Electronic Commerce Act III of 2001, the acceptance is effective upon the data message leaving the control of the sender. Other cyber laws provide that acceptance of the data message becomes effective only when it is received by the offeror or when it is in a situation in which the offeror has control of it and has ability to know of it (such as arrival into the email box of the offeror), whether or not the offeror actually sees it at that time i.e. .

The Namibian ECT Bill makes a provision that the contract will seems to be accepted when the data message of acceptance, of an offer, becomes effective, at the time and place it is received by the offeror.

It is my opinion that, if the contract is said to be formed at the time that the email was sent or at the time that the letter was posted, while the offeror is not yet aware. Then it will also true that when the offer is communicated to me, the offeror will be waiting for a response of an acceptance from me. Therefore I first have to make up my mind and be satisfied with whole offer's terms and condition as such. Secondly I need to decide that I will accept the offer as such or I will not accept it. Why not also the contract being formed at the time I have decided to

accept the offer even thought such (my) decision is not yet communicated to the offeror?

Mills (2003) stated that "As long as the laws of each jurisdiction differ in material ways from that of others, questions will continue to arise in interpretation and enforcement where there is any cross border element of an electronic transaction."

3.4 Legal Recognition of Data Messages and Contract Formation

Section 7 of the Namibia ECT Bill makes a provision that the "information must not be denied legal effect, validity or enforceability solely on the ground that is not contained in data message purporting to give rise to such legal effect, validity or enforceability, but is merely referred to in that message."

When the Namibian ECT Bill becomes an act, the data message is given a legal recognition, thereafter when a contract concluded online, will be legal in Namibia. This provision in Namibian ECT Bill is in line with section 107 of UCITA where "the record or authentication may not be denied legal effect or enforceability solely because it is in electronic form".

As information and communication technology advances, relevant laws and legal aspects dealing with ICT, needs to be redressed and revisited, to be able to deal issues on the cyber space. The Namibian ECT Bill is in par with international development, on its current format.

The Namibian ECT Bill makes a provision that; the submission of information in the data message will met the same requirement as if the information was submitted in the hard copy. This provision will make life easier for most of the people if not everybody. Imagine that, one may just apply online to a high learning institution within Namibian jurisdiction, for admission. One may also apply online for passport, birth

certificate or any other documents to the responsible Ministry or to any other government directorate, when the ECT Bill comes into a law.

Under the Namibian ECT Bill, when it becomes an act, where the law require information to be in writing, that requirement is met by the data message, provided that whoever needed the information, consented to received the information in the data message. Giving or providing information in the data message, include and will be not limited to, the following:

- making an application or lodging a claim,
- giving, sending or serving a notification,
- statement or declaration,
- lodging a return, making declaration or a demand, lodging or issuing a certificate,
- making varying or cancelling a election and lodging an objection and giving a statements of reasons.

3.5. Admissibility and Evidential Weight of Data Messages

Section 13 of the ECT Bill, make provision that in any legal proceeding, nothing in the application of the rule of evidence shall so as apply, to deny the admissibility of a data message in evidence: (a) on the sole ground that it is a data message, or (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on ground that it is not in its original form.

The Namibian ECT Bill makes also provisions that, based on the way the data message has been generated, created or retained, it will not be denied the evidential weight and the data message will be regarded equally as hard copy. The "way" or method the data message had been generated, created or retained should be clearly defined. There should a standard on how the data message should be created, generated and retained.

3.5 Conclusion

Once the ECT Bill is enacted the data message or information in the data message will have the same evidential weight or equivalent to the information in on hard copy.

Computer laws or Internet laws of different countries have been defined differently in terms online contract. This includes the online contract acceptance, formation of contract, etc. Irrespective to such different legislation, access to the internet is the same, hacking of computer seems to be the same and unauthorised of information seems to be the same but, we(world) still outlaw different cybercrimes and computer breaches different from one country to another.

Consensus may be reached to have consistency in the cyberspace as Mills (2003) concluded that "it seems patently clear that, because of the borderless nature of electronic commerce, the same can be regulated smoothly, safely and consistently on an international scale only if there is a single universal framework within which all legal systems will eventually operate."

CHAPTER 4: ELECTRONIC SIGNATURE

4.1 Introduction

It is a culture and a tradition that for any contract to be valid there should be a physical handwritten signature affixed to it. A signature is referred to as method used to identify a person or as method to indicate the person's approval of the information as communicated. May be the question will be is this achievable online? The answer might be yes; as there is electronic equivalence to the physical signature that is electronic signature or the advanced technology, referred to as secure electronic signature.

Electronic signature is already in use, in some countries, as Mills (2003) highlighted that "US President; Clinton signed a bill- electronically – giving full legal effect to electronic signature in the US. Apparently Hong Kong and New Zealand also have legislation recognising electronic signature and presumably most other jurisdictions have, or soon will have the same legislation."

The Namibian ECT Bill follows suit by making provisions for both electronic signature and secure electronic signature. The Namibian ECT Bill defines electronic signature as "means data in electronic transfer from, including an electronic sound, symbol, or process attached to or logically associated with a data message and executed or adopted by a person with the intent to sign the data"

The Namibian ECT Bill further defines secure electronic signature as "an electronic signature duly recognised in terms of section 10 of the Namibia ECT Bill.

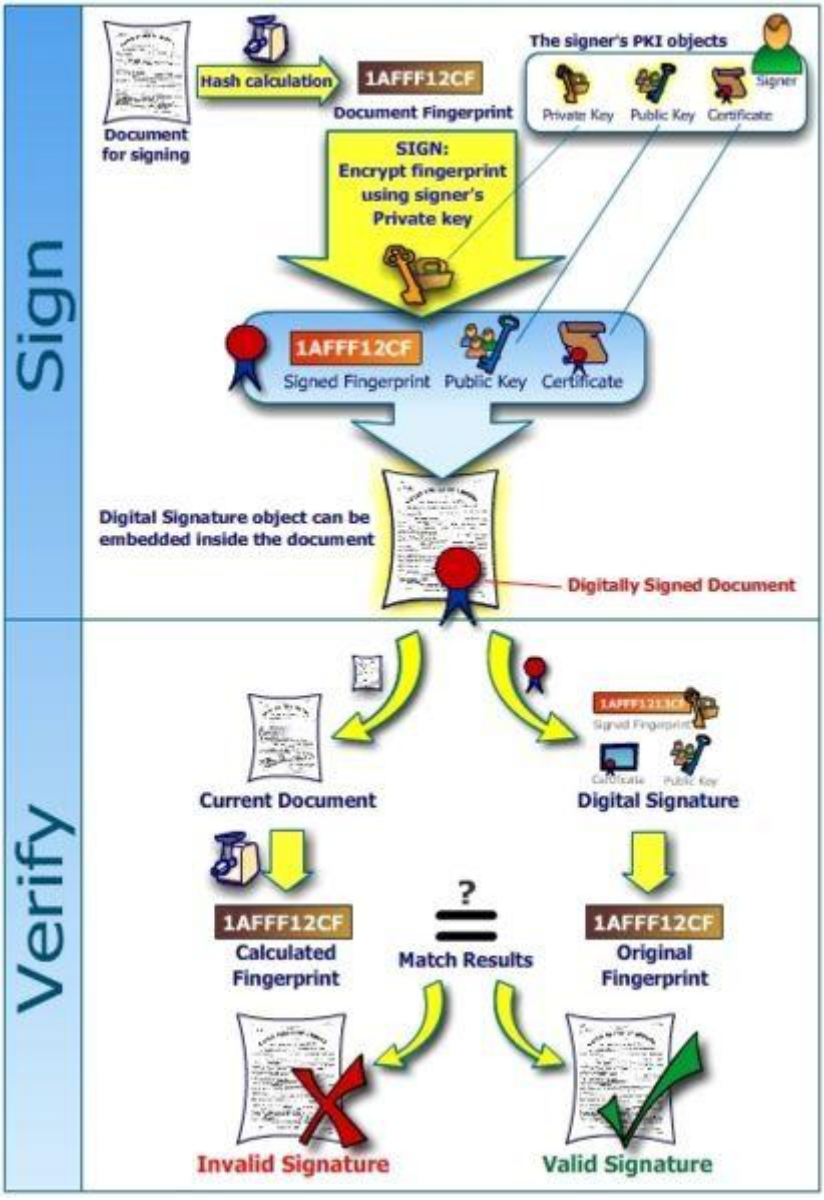
The electronic signature is created and can be verified through the application of a security procedure or combination of security procedures that ensures that such electronic signature:

(i) is unique to the signer for the purpose for which it is used;
(ii) can be used to identify objectively the signer of the data;
(iii) was created and affixed to the data message by the signer or using a means under the sole control of the signer; and;
(iv) was created and is linked to the data message to which it relates in a manner such that any changes in the data message would be revealed."

The provision of electronic signature in the Namibia Electronic Transaction Bill will eliminate repudiation by the parties to the contract when such contract is signed electronically, in case disputes arise between the parties.

Non-repudiation is the concept of ensuring that a contract cannot later be denied by either party involved in forming that contract. With regard to digital security, non-repudiation means that it can be verified that the sender and the recipient were, in fact the parties who claimed to send and receive the message respectively.

Below is a demonstration on how the digital signature can used or applied:
"Since they've noticed the villainous Eve trying to interfere with their communications, Alice and Bob have started using very short-lived keys. Now Alice needs to send a message to Bob, but this time she needs to be able to prove not just that she was indeed the sender, but she also must be able to prove *when* the message was sent, so that Bob knows her key was valid at that time. Equivalently, once Bob knows all of the above, Alice can never deny (or repudiate) having sent the message; this is where non-repudiation gets its name.(Coombs, 2006)"



A diagram showing how a digital signature is applied and then verified.
Source:http://upload.wikimedia.org/wikipedia/commons/b/b5/Digital_Signature_-_How_it_works.jpg

4.1.1 Certification Authority and Issuing Authority

Introduction

The Namibian ECT Bill does not make a provision for the certification authority or issuing authority, as in the case of South African ECT Act. Chapter six (VI) of South African ECT Act of 2002, make a provision the Accreditation authority. The functions of the Accreditation Authority

include monitoring the conduct and operation of the authentication of service provider to comply with certain requirement of the cyber laws in terms of managements of electronic signature.

"Abbreviated as CA, is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be ("Certification Authority", 2007).

Again there still some issues as far as digital signature is a concerned. Barnett (2001) further noted that "legal issues with respect to digital signatures are not easy to address since the digital world moves quickly and legislation and technology are constantly playing cat and mouse. Unquestionably, e-business will not meet its full potential unless there is a secure system(s) in place to confirm the accuracy and authenticity of electronic signatures."

The Namibian ECT Bill makes a provision for the electronic signature but it does not make any provision for the Certification Authority. The Namibian ECT Bill also does not make a provision on how to authenticate the secure electronic signature.

Sections 10 and 44, of the Namibian ECT Bill, make the provision that a responsible Minister may make a provision of a regulation regarding any matter concerning the licensing and standards of secure electronic signature. The issue of secure electronic signature may be dealt by the regulation by the Minister on the advice of the Electronic Information Systems Management Council (EISMC), as provided for in the ECT Bill.

4.2 Overseas adoption of digital signatures

Other states worldwide have made similar provisions by making the law specific for electronic signature or digital signature. States overseas

have passed legislations to implement digital signature processes. Some of those legislations are listed here below:

1. the Digital Signature Act 1995 (Utah);
2. the Digital Signature Act 1997 (Federal Republic of Germany);
3. the Electronic Communications Act 2000 (United Kingdom); and;
4. the Electronic Signatures in Global and National Commerce Act 2000 (United States of America).

Notably, President Clinton led the trend in signing the Act using both his hand-written and electronic signatures.(Barnett, 2001)

Barnett (2001) pointed out some issues with the digital signature by listing some advantages of electronic signatures as follows:

1. access to market places,
2. less paper storage,
3. better security,
4. minimum outside security and;
5. better certainty of security.

Barnett (2001) also listed the disadvantages of electronic signatures listed as follows:

1. problem with simplicity,
2. problem with control,
3. problem with access and problem verifying and;
4. problem with deterioration.

Namibia has made provision for the digital signature in the ECT Bill. Other states have gone another step further by coming up with additional or separate legislation(s) only dealing with digital signature. As long as there is no way to forge the electronic signature electronically, it will be safe to use the digital signature. But it is possible to forge the electronic signature that is why the Certification Authority is a necessity.

Mills (2003) points out that "Jurisdictions which adopt the MLESig, preferably together with the Model Law, will have accepted electronic signatures as, more or less, the equivalent of a physical signature on paper. However, it does not provide any guidance as to how the electronic signature may be created to meet the requirements." This might be left to the individual state take it further on their own.

Electronic signature should be created securely and should meet the standard requirement in terms of security. An example should be learnt from the state(s) or country which has enacted similar law and legislation i.e. the United State of America. The stumbling block might be the cost, skills, knowledge and the capacity to come up with all the requirements for the implementation of secure electronic signature, especially in African countries, Namibia included.

In Namibia, once the ECT BILL is enacted, the option is provided for the relevant ministry to come up with the Certification Authority by means of regulation.

4.3 CONCLUSION

The development and effort to make digital signature and data message having evidentiary weight equivalent to hardcopy is another step in the right direction. The two (digital signature and data message) will be acceptable and admissible in the court of law. There will be no time for anybody to go in personally, to any offices, just for the physical signature that is needed on the transaction. The digital signature or an email with a proper identification should be adequate to communicate the approval required.

Namibia should make a provision for the procedures to deals with the secure system for electronic signature. This system should be in place at the time the Namibian ECT Bill is enacted. The current format of the Namibian ECT Bill is in line with development worldwide. Those with

signing authority will sign document online and the decisions or business transaction will be done quicker to the benefits of both customers and businesses.

CHAPTER 5: OTHER LEGISLATIONS CONSIDERED

5.1 Introduction

This thesis has considered some cybercrime legislations and ECT acts from countries worldwide. These legislations were benchmarked with Namibia ECT Bill. This research found out that it is evident that each country outlaws whatever it feels like and proper to criminalise, based on its physical boundary. This is despite the fact cyberspaces knows no limits of physical boundaries.

The ECT acts or Computer Acts that was considered during this research are:

1. The Computer Misuse and Cybercrime Act 2003, (Mauritius).
2. Data Protection Act (Act XXVI of 2001, as amended by Act XXXI of 2002)(Malta).
3. Northern Territory of Australia – Electronic Transactions (Northern Territory) Act 2000.
4. Electronic Communication and Transaction Act, 2002 (South Africa).
5. Malta Electronic Commerce Act -ACT III of 2001, as amended by Acts XXVII of 2002 and IV of 2004.
6. The Data Protection Act 2004 – Act No. 13 of 2004.C
7. Cybercrime Act 2001, No. 161, 2001, (Australia)
8. the Prevention of Computer Crime Act, No. of 2003 (Sri Lanka)
9. The Uniform Computer Information Transaction act. (Enacted in Virginia)
10. Computer Misuse Act of Singapore

The computer acts or laws above have been studied and evaluated with the purpose to be compared with Namibian ECT Bill. Even thought the Namibian ECT Bill is in line with most of these laws, there are some differences in comparison. This is not only unique to the Namibian ECT

Bill but with some other acts from one country to the next. The differences are mostly on how the each country defined and regulated its own law i.e. acceptance of contract, unauthorised access, criminalised internet activities, etc.

5.2 Differences in defining and outlawing cybercrimes

The figure below shows what is covered and what is not, in some selected Asian countries' cyber law. These countries' cyber laws do differ in much extent that they did not address the some online activities. Cybercriminal(s) may see this as loophole to carry out their criminal activities and as safe heaven to avoid being prosecuted.

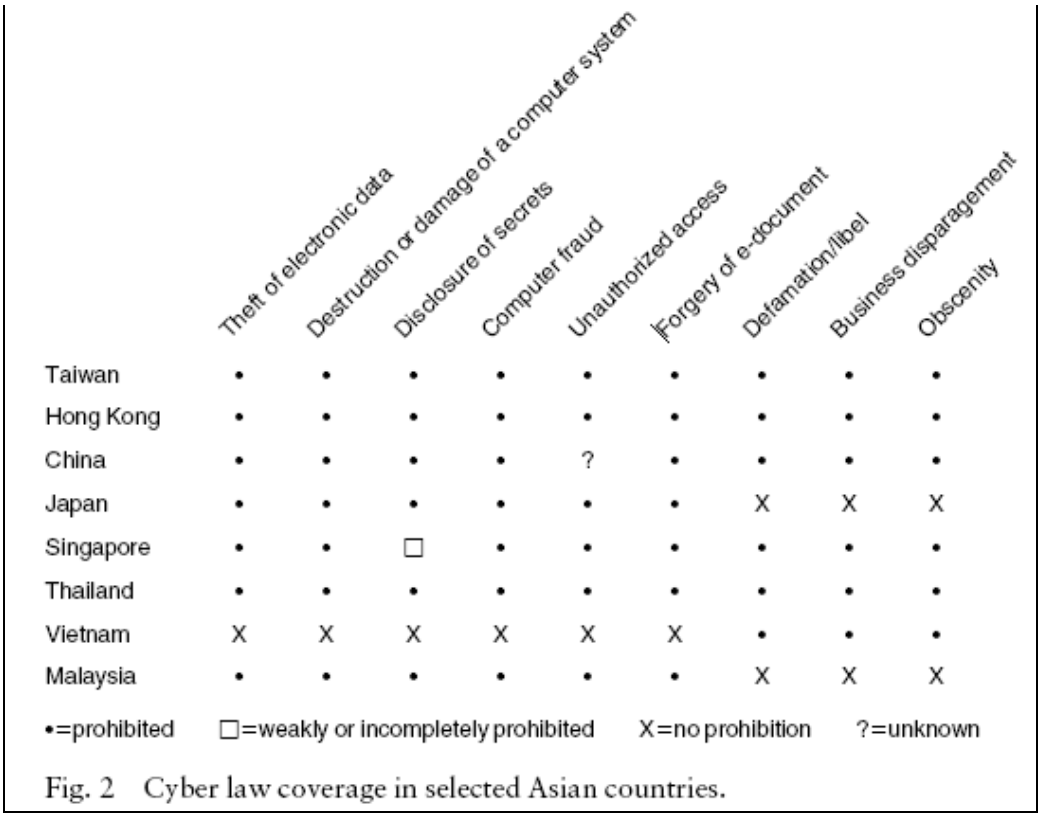


Fig 2: Cyber Law coverage in selected Asian countries.
Source: http://media.hoover.org/documents/0817999825_35.pdf

Putnam and Elliott (2001) noted that "under Taiwanese law, merely accessing a computer system without authorization would not be considered as an offense unless there was also a proof of an additional

crime, such as modification or destruction of data, while under Japanese law, unauthorised access to a computer in which an individual may view secret information is itself a criminal offense, even if there is no damage to the system"

I tend to disagree with the provision in the Taiwanese law, that access without permission should not be an offense. Unauthorised access should be a criminal offense as it is, in the Japanese law. What if somebody access the computer system without the authorization and view the confidential information without modifying or destroying them?

Section 33 of the Namibian ECT Bill makes provision for an unauthorised access to an information system, as a crime. This provision is similar to the Japanese law.

The possibility exists that the effect of cybercrimes and computer breaches will have an impact equally on all countries connected to the internet. Given the example of Love Bug, the Philippine authority was faced with the problem of arresting a suspect, and not to mention the conviction of the suspects in the court. It is high time that cybercrimes should be defined and covered the similar in each and every country.

5.2.1 Some Comparisons

5.2.1.1 Data Message Recognition

The recognition of data messages is provided for in the Namibian ECT Bill. Nothing similar is provided for in the Mauritius Computer Misuse and Cybercrime Act. Malt has made the same provision (Malta Electronic Commerce Act) that information in writing is met by submitting the same information by means of electronic communication.

5.2.1.2 Age Limitation for Legal Purpose

Watney (2005) stated that "The Convention on Cybercrime recommends that a minor should include any person under age of 18 years but indicates that that a signatory country may require a lower age limit but it may not be less than 16 years."

In comparing the age limit, Chawki (2005) highlighted that "The age of the children protected by the laws against child pornography differs considerably: When it comes to protecting minors from being exploited as actors, the age limit is 14 years in (Germany and Austria), 15 years in (France and Poland), 16 years in (Switzerland and the United Kingdom) and finally 18 years in (Sweden, and the US)"

Most countries have made a provision for age limit at 18 years, while this is different from other countries. From the table below, different countries have different age limit in different aspects of life.

Age limit for	Namibia	Germany	Denmark	South Africa
Marriage Consent	21	18	18	21
Sexual Activity Consent	16	14	15	No specific age defined
Simple Age Majority	21	18	18	21

Table1:. Age limits comparison in different countries.

The situation in Scotland is different, as it is highlighted below, on how the age limit is defined. According to MacDonnell (2007), at each age limit, one is allowed on what to do at each different age and what not.

MacDonnell (2007) highlighted that "At the age of 16, in Scotland one can or is allowed to do the following: .i.e. get married, have sex, join the armed forces, but not fight on the front line, start your own business and

become a company director, drink alcohol - but only beer and cider with a meal in a licensed premises, leave school, pay taxes, be employed full-time and pay adult fares on public transport" .

"While at the age of 17 one is allowed to learn how to drive a car and while if become 18 years old you are allowed to fight on the frontline in the armed forces, to participate in voting process and also to buy alcohol and drink it." (MacDonnell, 2007)

5.2.1.3 Age limit on Cyberspace

The Convention of Cybercrime recommends that a minor should be considered a person under the age of 18 years. With the minor age limit defined differently from country to country, this will create problem in the cyberspace legislation. A notable example is the website in Germany which was catering for an adult market.

According to Brenner and Koops (2004) "the website finds itself indicted in Singapore, because of spreading pornographic material in Singapore. To make things worse, the Web site owners are ordered to appear in court in Belgium, because some of the adult pictures are considered to be of 17-year old minors, constituting the crime of child pornography (which, in Belgium, entails persons under 18 years of age; in Germany, the age limit is 14)"

From the above scenario, one could see that given the cyberspace, conflict will always be there. The anticipated single universally cyber law may solve the conflict, created by different provisions in cyber laws.

5.2.1.4 Child Pornography as Crime

Not all states have "child pornography" as a crime in their domestic laws. The children need to be protected by all means from whatever

type of unlawful activities on the internet. Namibia has a provision, in the ECT Bill, for child pornography even though in comparison to the USA, it seems to be less effort. USA has more than three acts just for the protection of the child against pornography in the cyberspace.

Information and Communication Technology is advancing at a fast pace, therefore, the ECT Act need to be updated on regular basis, in order to protect and counter illegal activities on the internet. Kowalski (2002) points out that "It was already illegal in Canada to possess child pornography, but revisions were made to legislation to make it illegal to download and view child pornography online.

Wortley and Smallbone (2006) stated that "because of the increasing use of computers in society, most police departments are likely to encounter Internet child pornography crimes. Therefore, it is important that all police departments develop the strategies on how to dealing with the cyber crimes."

The International Centre for Missing & Exploited Children carried out a study, in 2006, on child pornography and the result were shocking. The study was carried out in 184 Interpol member countries, on which Namibia is also a member and was included in the survey.

The table below tell a lot on how each country has defined its law with regards to the child related pornography.

Country	Legislation Specific to Child Pornography	"Child Pornography" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Mozambique	✗	✗	✗	✗	✗
Myanmar	✓	✗	✗	✗	✗
Namibia	✗	✗	✗	✗	✗
Nauru	✗	✗	✗	✗	✗
Nepal	✓	✗	✗[47]	✗	✗
Netherlands	✓	✓	✓	✓	✗[48]
Netherlands Antilles	✗[49]	✗	✗[50]	✗[51]	✗

Fig. 5.2.3a Global Legislative Review: Child Pornography.
Source: Copyright © 2006, International Centre for Missing & Exploited Children

The study did evaluate the child pornography laws, in those countries by considering the following five criteria:

1. Are there existing laws criminalizing child pornography?
2. Does existing law include a legal definition of child pornography?
3. Is the possession of child pornography a crime?
4. Is the distribution of child pornography via computer and the Internet a crime?
5. Are Internet Service Providers (ISPs) required to report suspected child pornography to law enforcement? "

The finding of the study on the following figures below, with only few countries which have met all the criteria used in the study. Based on the result, Namibia is among the category of those countries which do not have child pornography legislation to protect the children against online pornography.

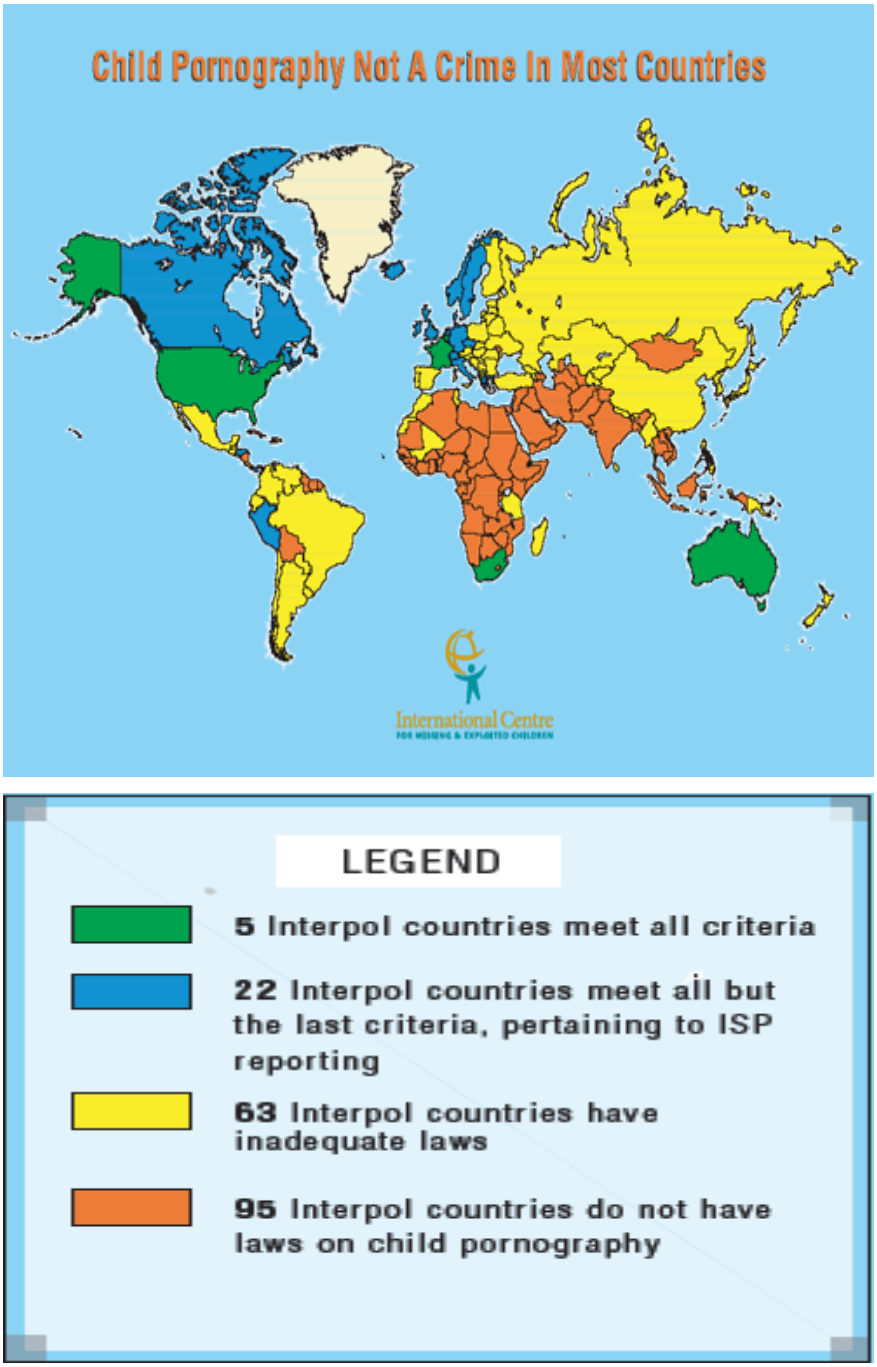


Figure 5.2.3b: Child Pornography not a crime in most countries
Source: **http://www.missingkids.com/en_US/documents/CP_Legislation_Report.pdf**

The result of the study shows that Namibia is lacking strong and adequate provision for the child pornography. Child pornography is current catered for, in the Namibian ECT Bill, and it will be defined as a part of the Namibian law once the ECT Bill is enacted.

5.2.2 A USA Approach about protecting the Child

In an attempt to cater for all aspects in combating child pornography, US have come up with some acts like:

1. Communication Decency Act (CDA) of 1996,
2. Child Online Porn Act (COPA) of 1998,
3. Children's Internet Protection Act (CIPA) of 2000; and
4. The Child Obscenity and Pornography Prevention Act (COPPA) of 2002.

The table below highlights the development of the child pornography laws for the protection of the child in the United State of America.

Table 1: Development of child pornography law in the United States		
Date	Legislation/Ruling [7]	Comment
1978	Sexual Exploitation of Children Act	First federal law specifically dealing with child pornography. Prohibited the manufacture and commercial distribution of obscene material involving minors under 16.
1982	New York v. Ferber	Child pornography not protected by the First Amendment. Child pornography separated from obscenity laws, to be judged on a different standard.
1984	Child Protection Act	Age of minor covered by child pornography legislation was raised to 18, and distinction between child pornography and obscenity codified.
1986	United States v. Dost	Expanded the definition of child pornography to include sexually suggestive depictions of a lascivious nature.
1988	Child Protection and Obscenity Enforcement Act	Illegal to use a computer to depict or advertise child pornography.
1990	Osborne v. Ohio	Private possession of child pornography ruled to be illegal.
1996	Child Pornography Protection Act	Definition of child pornography expanded to include virtual images of children and images that appear to be of a minor.
1998	Child Protector and Sexual Predator Punishment Act	Internet Service Providers (ISPs) required to report known incidents of child pornography to authorities, but not required to actively monitor customers or sites.
2002	Ashcroft v. Free Speech Coalition	Virtual images ruled not to be pornography; 'appear to be a minor' ruled to be too broad.

Table 2: Development in the US on child pornography.
Source: http://www.popcenter.org/problems/child_pornography/

"It is of particular importance that children online should be given adequate protection, which can only be enforced by suitable legislation" (Jahankhani, 2007).

Freedom of Expression is guaranteed in the USA; therefore, as a result it may have contributed to USA coming up with more than one child act.

From The International Centre for Missing & Exploited Children's study in 2006, it no wonder why the USA is among the states, which nearly met all the criteria used in the research. USA nearly met all criteria by having more than three acts, all about protecting the child.

"One of the reasons to come up with more than one laws in this regards was that the definition of indecent material was rather vague in the CDA and the COPA, which were aimed to restricting material that is harmful to minors" (Nel, 2004, Cyberlaw@SA).

5.3 Cybercrime Statistics

Research on cybercrimes and computer breaches carried out by the Australian Computer Crime and Security, has found out that statistics recorded might not be a realistic figure. According the research, not all company or organisations are reporting every cybercrime and computer breach, which they are faced with or they did, came across.

Goodman and Brenner (2002b) states that "Some of the reasons for the under-reporting of cybercrime are that "victims may not realize that the conduct involved is a crime, or may decide not to complain for reasons of embarrassment or corporate credibility."

Nemerofsky (2000) has stated that the cybercrimes static's has never been accurate. He pointed out that: "Although there has never been accurate nationwide reporting of computer crime, it is clear from the reports which do exist . . . that computer crime is on the rise."

Grabosky (2000b), stated that "some of the most deftly perpetrated offences with or against information systems are never detected, not

even by their victims; of those which are, some are concealed from authorities because disclosure could prove embarrassing or commercially inconvenient to victims."

Furthermore, Kowalski (2002) stated that "in addition, cyber crime may be one of the most under-reported forms of criminal behaviour because the victim often remains unaware that an offence has even taken place and in the case of businesses, are reluctant to report for fear of loss of consumer confidence."

This issue of not reporting the cyber crimes was also confirmed by another research done by the CSI/FBI in 2005. From this research it can be seen that organization avoid the negative publicity and afraid that competitors would use the information to their advantages if it is become known by them, thus will hurt their organization's stock and/or image.

The CSI/FBI (2005) survey found out that, "the claim of being unaware of law enforcement's interest in the breach was also cited by 16 percent, of the respondents, as a very important reason for failure to report the intrusion."

Even though from the survey done, the statistic is increasing, the figure might change as it seems that not all cybercrimes are reported and subsequent recorded as such. The implication is that the cybercriminals go free unpunished and without facing the law.

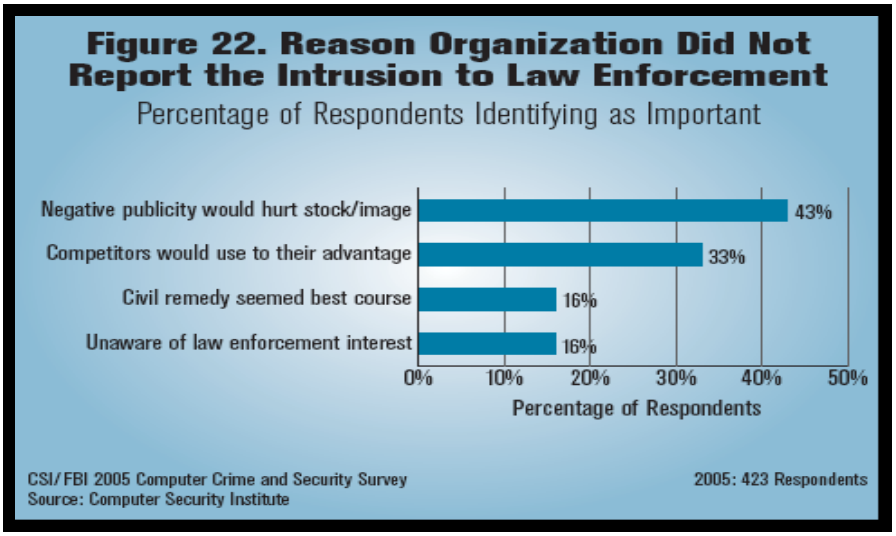


Figure 5.3a: Reasons why Organizations did not report the intrusion to law enforcement
Source: Computer Security Institute (USA)

A lot still need to be done by countries if cyber crimes and computer breaches should be combated and prevented at all cost. Countries all over the world must cooperate on strategies on how to counter and prevent cybercrimes. The Convention on Cybercrime needs to be extended to all countries willing to become a signatory to it. This mean that each country wish to became signatory to the Convention on Cybercrime, should do so freely.

It is not prohibited, for any country to define its cyber law in a similar manners or ways as the Convention on Cybercrime.

5.3.1 Law Enforcement Authorities

The law enforcement authority normally refers to the national police force, in any given states. Is such law enforcement authority having the capability of dealing with the newly emerging crime committed with computers? Kowalski (2002) pointed out that "One of the challenge currently faced by legal authority is the difficulty of applying existing legislation to criminal activities involving new technology"

Putnam and Elliot (2001) had argued that "The enforceability of laws against cyber offenses enacted at the national level becomes

complicated when, as is frequently the case, the source, object, or path of an attack has its physical nexus in more than one country."

The law enforcement authorities should be well equipped with all the necessary skills, knowledge and with right equipments. This will help the staffs of such authorities to combat and prevent cybercrimes. Organisations, businesses and public at large must have confidence in the law enforcement authorities. This is possible if the law enforcement authorities demonstrate that they are indeed capable of tackling and preventing cybercrimes.

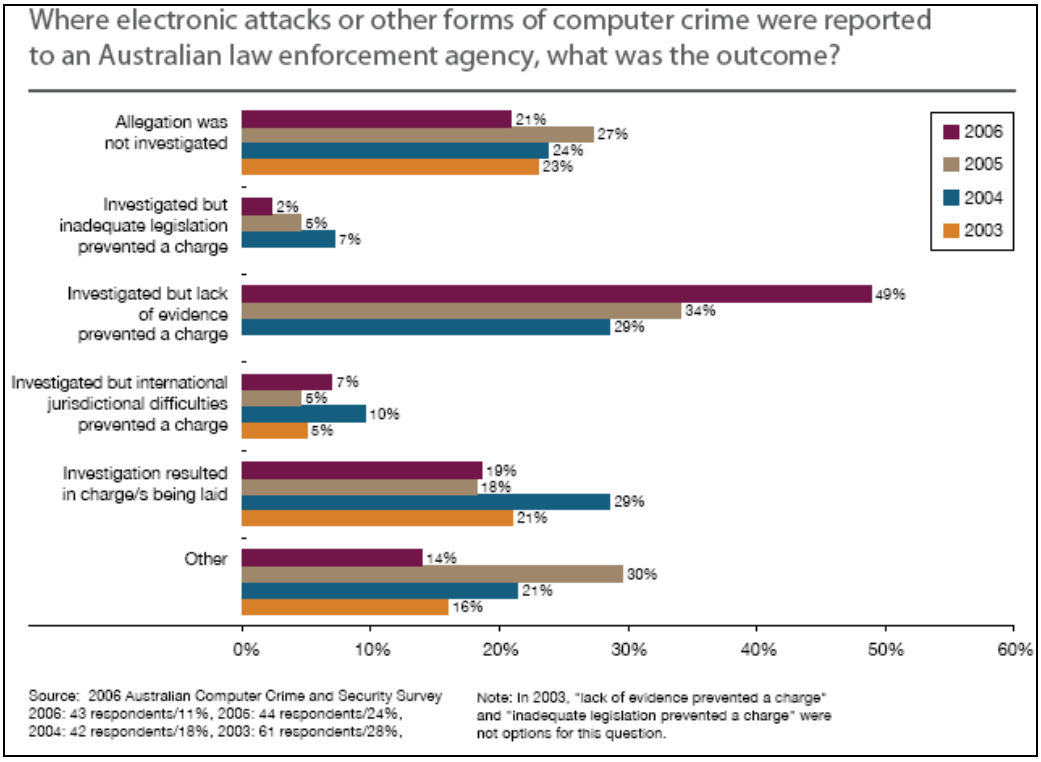


Figure 3: What happen when the case was reported, in this case to the Australian law enforcement agency?

5.4 Cyber Laws of Nations / School of Hacking

Jones (2005a) points that according to Ken Dunham, director of malicious code at iDefense in Reston, Virgina, warned that "In Russia, perhaps more than in most other countries right now, hacking

magazines and software are sold on the streets of Moscow…It's not a secret as you'd expect, but right out there in the open." Moscow boasts a Civil Hackers School (http://hscool.net/), which claims to teach "legal" hacking activities.

The author of this research is of the opinion that "YOU CAN BUT YOU MAY NOT". You may learn how to hack but you must not hack into others computers or network. Knowledge and skills of how to hack is required so that, counter measure may be taken to prevent it.

Schools of hacking will be nice and helpful for the law enforcement authority, as they need to know, to have skills and knowledge in all activities happening in the cyberspace. How are they going to do investigation without the necessary knowledge, and how are they going to catch and arrest the hackers? How are they going to convince the court, for the suspects to be convicted, if the men and women in uniform do not have skills and knowledge in hacking?

One may attend a shooting school, but that does not mean after the lessons, s/he must start shooting at whatever come on sight.

5.5 Dual/Double Criminality

The Double criminality refers to a punishable offence committed in country A by the suspect in country B and the same offences is also a punishable offence in country B. In this case it is easy to extradite the suspect to country A in order to stand a trial there.

Jones (2005b) pointed out that "although the Convention allows Parties to refuse requests for mutual assistance on dual criminality grounds – provided they have such requirements in current mutual assistance regimes – it does not require that they do so. It does allow them to refuse cooperation if the offense is "political," but these groups desire more detailed explanation for what qualifies as a "political" offense".

When US wanted the two men from Russian, Russia did not cooperate with US to hand over the two men to stand a trial in the USA. Philippine was willing to assist and cooperated in the case of Love Bug. But due to lack of inadequate legislation there was nothing much Philippine can do to help other countries which wanted to extradite the Love Bag suspect.

The Philippines were faced with dilemma whether to prosecute the "Love Bug" suspect. Subsequent they quickly adopted legislation outlawing certain types of cybercrime including the creation and dissemination of viruses (Goodman and Brenner, 2002b).

Namibian ECT Bill did not make provision for online auction fraud. Goodman and Brenner (2002a) stated that the online auction fraud is one of the most common types of cyber fraud. How will Namibia deal with online auction if there is no provision on the ECT Bill?

And another concern is how Namibia will deal with dissemination of hate and racist speech or related issues, given the guarantee of freedom of speech and of expression in the Namibian constitution.

5.6 Single Universal Framework

It seems to me that there is no urgency towards adopting and coming up with the single universal legal system. The world will be forced by the situation to move toward the universal legal systems; as cybercriminal will take advantage of safe heaven country. One of the good examples is the age limit defined differently from country to country. A person in Namibia may view the image from another country where the age limit is differently defined, which will not be illegal in that specific country.

I agree with Watney (2007a) when stated that "Countries paid little or no attention to the legal regulation of similar issues in other countries. Countries implemented legal regulation of the internet without giving any regard to the enforcement of the internet laws."

According the working group, which is responsible for drafting the Namibian ECT Bill, on ECT BILL acknowledged unlawfully activities in cyberspace, despite acceptable but often untested present – day definitions, should carry criminal liability. Again in this connection, present-day international practise and pretended provide the basis for Namibia to also adopt similar provisions by ways of law.

Burke (2000) stated that "The call for global laws to govern the Internet has been raised once again in the wake of the Philippine government decision to drop all charges against the "Love Bug" suspect, Onel de Guzman."

5.7 CONCLUSION

It is not enough that any country should defend itself from the threat of cyber criminals alone, without the help of other countries. This need effort and involvement of all stakeholders in the cyberspace. Watney (2007a) stated that "The challenges of electronic medium cannot be resolved without the involvement of the law and in many instances, cooperation between various countries are needed to address legal problems such as copyright infringement and cybercrime."

If possible, all countries should ratify the European Convention on Cybercrime, even though their domestic law might be the stumbling block in achieving this. USA is one good example where the existing domestic law will be violated if they ratify the Convention on Cybercrime in full i.e. First Amendment which guarantees freedom of speech.

It high time that World needs to come up with single universal law to govern and regulate the activities in the cyberspace. This single universal law should be part of each country's domestic law. However dilemma is how to address and convince some countries to change and amend their domestic laws to, support the single universal law which govern the cyberspace.

CHAPTER 6: CYBERSPACE JURISDICTION

6.1 Introduction

"Jurisdiction is the power or authority and right to enforce or apply the law in a territory or for a court of law to hear decide on the specific case brought before it" (Hamano, 2000).

The question in this regards is that, will the Namibian court has jurisdiction on a crime committed outside its border, but have effect inside Namibia.

Rustad and Koenig (2005) stated that "the Internet raises unique jurisdictional issues because this new technology respects no national borders. Cyberspace raises inevitable jurisdictional issues because, by its very definition, the Internet involves trans-border communications across hundreds of countries at the click of a mouse."

Hamano (2000) stated that "according to traditional principle, jurisdiction can be divided into three categories:

1. Jurisdiction to prescribe or Legislative jurisdiction
2. Jurisdiction to adjudicate or Judicial jurisdiction
3. Jurisdiction to enforce –or Executive jurisdiction"

Hamano (2000) further defines the three types of jurisdiction as follows: **"Jurisdiction to prescribe"** means a State's authority to make its substantive law applicable to particular persons and circumstances

"Jurisdiction to adjudicate" is defined as a State's authority to subject persons or things to the process of its courts or administrative tribunal, whether in civil or in criminal proceedings, whether or not the State is a party to the proceedings

"Jurisdiction to enforce" deals with a State's authority to induce or compel compliance or to punish non-compliance with its laws or regulations, whether through its courts or by use of executive, administrative, police, or other non-judicial action

Goodman and Brenner (2002a) pointed out that "inconsistent national criminal laws were acceptable so long as crime was parochial. A nation's decision whether to criminalize activities was a matter solely within national discretion because the consequences of that decision would impact only upon those living within its borders, generally its own citizens." This being not the case anymore, as terrestrial border is now irrelevant because of the use of the internet.

Section 41(b) of the Namibian ECT bill makes a provision that irrespective of wherever the offence have been committed from, as long as it have effect in Namibia, then our court has jurisdiction over that offence. This provision may be enough as long as jurisdiction over the offences which are committed in Namibia. What about the decision of Namibian courts, to be enforced outside Namibia?

When referring to the Malaysia 's computer act, Brenner and Koops (2004) pointed out that "the Malaysia's Computer Crime Act is even less limited than Singapore's":(1) The provisions of this Act shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia

This provision for Malaysia is quite well defined. It makes provision for jurisdiction for Malaysia court to try criminal even if they have committed the crime outside Malaysia, which have effect in Malaysia. This will only be effective with the cooperation with other countries, as

similar provision in other countries' cyber laws, has proved to be useless i.e. Yahoo cases, Love bug case, DVD case, etc.

Carey (2000) stated that "Internet and other electronic transactions take place without physical presence in the place where the activity may have significant effects. When is it fair and appropriate to assert jurisdiction?"

The answer to this question is that countries that are both affected by the online activities need to cooperate provided that their cyber laws are similarly defined. Countries should not wait until they are affected by cybercrimes before they criminalize certain activities in the cyberspace. States should instead learn a lesson from those countries that have suffered consequences because of inadequate laws and thereafter they take a reactive step.

Brenner and Koops (2004) pointed out that "Jurisdiction to adjudicate is a sovereign entity's authority to subject persons or entities to the process of its courts administrative tribunals" for the purpose of determining whether prescriptive law has been violated.

The issue is when one country's cyber law criminalise the computer-related crime, while other country's does not outlaw such crime. The possibility of extraditing the suspect(s) may not be possible, as it was experienced in case of the Love bug.

Due to differences in culture and social, the freedom of speech can be seen as a misuse in some countries. The Nazi items displayed on the website of Yahoo! Inc, which available online and accessible to a French citizen was legal to display in USA, whilst not in France. What is ethical and acceptable in one country might not necessarily be ethical acceptable in another country. Information on the internet is available to any people whom are connected to the internet irrespective of physical location.

6.2 Approach to Jurisdiction

Some concerns that need to be addressed are to what extent, when a county ratify the Convention on Cybercrime, will do the damage to ones' domestic law? I am raising this question as most of the countries have not yet fully ratified the Convention on Cybercrime and some have yet not a law in place similar to the Convention' s provision.

Cox (2006) state that according to Article 2 of the 2001 Council of Europe's Convention on Cybercrime required signatory governments to enact such provisions as may be necessary to establish as criminal offences under their domestic laws, when committed intentionally, the access to the whole or any part of a computer system without right.

6.2.1 Ratification of the Convention on Cybercrime

The purpose of the Convention on Cybercrime is to facilitate the international cooperation in the investigation and prosecution of computer crimes or crimes that are committed in the cyberspace. This was necessitated by the procedural and jurisdictional obstacles, which in practices have been observed by delaying the investigation of cybercrimes. Sometimes it even delays the prosecution process of those responsible for computer-related crimes.

Referring to the Convention on Cybercrime, McIntyre (2005) had stated that "Some of the most deftly perpetrated offences with or against information systems are never detected, not even by their victims; of those which are, some are concealed from authorities because disclosure could prove embarrassing or commercially inconvenient to victims."

For a country to become a signatory to the Convention on Cybercrime, it must be invited by the member state. I wonder why, non-member

states to the Convention, should not be provided an opportunity to approach the member state, for the recommendation to be a signatory to the Convention.

Calvert (2005b) pointed out that "securing the cooperation of those countries that has not yet signed the European Convention on Cybercrime is critical as such countries are arguably the most likely to act as safe haven for cyber criminals."

Definitely member states will only invite the state of their choice and mostly if there is interest and any other reasons do to so. Otherwise what will be the motivation for the member state to invite non-member to join the Convention? It is my opinion that states that wish to become a signatory to the Convention should do so freely and at will.

Magnin (2001) stated that "The other non-Council of European States participating in the negotiations are: Canada, Japan, and South Africa. By virtue of their having participated in the Convention's elaboration, the United States and these other non-CoE States will have the right to become parties to the Convention if they choose to do so."

Li (2007) had also emphasized that "However, apart from the fact that it represents a significant step forward, more states will have to sign the Convention and abide by its mandates in order to serve as a deterrent."

The European Convention on Cybercrime is not discriminatory under any circumstances to any country neither it is replacing any existing legislation. But some countries still feel that the Convention violates their domestic law if they have to ratify the whole Convention.

I agree with Magnin (2001) when he stated that "The Council of Europe Convention on Cyber-crime is the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks." If more countries join the Convention, it will increase and secure the cooperation in combating cyber crime worldwide. The growing of the Convention on Cybercrime members will be a strategic step toward a solution to a jurisdiction problem.

This was also emphasised by Mills (2003) that "There is no government with the jurisdiction to govern or regulate cyberspace. Only if all governments adopt the same laws to govern "e-economic" transactions will there be the possibility of an even playing field and effective, transparent, flow of business through the internet. Otherwise a transaction may be subject to too many, conflicting, laws, or perhaps to none at all."

The above point is clear that the solution to combat and prevent cybercrime lies with cooperation of governments worldwide. I think this approach will help to reduce the cybercrimes jurisdiction dispute. This will create a solid basis for law enforcement authorities to cooperate with their counter parties in combating the crimes committed in the cyber space.

6.3 Jurisdiction Conflicts

It will be good and helpful if all the cybercrime legislation should try to resolve and avoid conflict when it occurs, in terms of cybercriminal prosecution, cybercriminal extradition and cyber jurisdiction. But how is it possible to achieve this, if what is illegal in my country is legal in another country?

I believe there is enough evidence of jurisdiction conflicts. Enough evidences for the states of this world to cooperate, toward narrowing the gap on cyberspace jurisdiction conflict. One of the examples is the

emails send from adolf@hitler.com, which sends email via server in the USA. The Germany could anything to continue with investigation due to domestic laws of USA (Goodman and Brenner (2002a)).

In the absence of a single universal law governing cybercrime, jurisdiction conflict will be here to stay. Goodman and Brenner (2002a) state that "mechanisms of cooperation across national borders, to solve and prosecute crimes are complex and slow." This should follow up with cooperation and similar legalisation of all possible cybercrime outlawed by all nation/states

Another dilemma to solution on cybercrime jurisdiction is the domestic law of some countries. According Magnin (2001); it is fact that "the United States have widely provided their expertise and given their opinion during the deliberations related to the COE Convention on Cyber-crime. This participation has enabled the United States to prevent the adoption of important amendments like the criminalization of "racists" websites that, in the US point of view, is contrary to the U.S. Constitutional Protection of Free Speech."

6.3.1 Action that have effect on its territory

This clause "has an effect on its territory" has become a common clause to most ECT acts. In the Namibian ECT bill as well, the court will have jurisdiction to any crime that has an effects in Namibian territory.

There are cases where country B is claiming jurisdiction on cybercrime committed in a foreign country A. But in country B where such action did take place, is not a crime. Subsequent by law, country A will not cooperate to render assistance to country B.

This clause will be useless in the absence of the universal frame work toward a single law governing cyber crimes. The clause will be irrelevant as countries are reluctant to change their domestic laws to be in line with Convention on Cybercrime.

6.4 Solution to Jurisdiction

All cyber crimes should be defined the same way in each and every jurisdiction. Whatever is the crime in the cyberspace should be outlawed in all countries of the world. It is a fact that cybercriminal can study the cyber legislation of each and every country. Once getting familiarizes with certain cyber law, they may take the advantages of the loopholes in such legislation.

Jurisdiction conflict will be avoided by putting appropriate tool in place. Magnin (2001) stated that "The only appropriate tool to fight them(cyber criminal) is by enacting new Laws, harmonize international legislations and encourage coordination and cooperation between national law enforcement agencies"

The potential do exist that cybercrimes may be committed from a country where it is not define as a crime, to the victim country. A good and notable example according to Goodman and Brenner (2002a) is quoted below: "The e-mail address of a group of Jewish students in Germany was bombarded with more than 17,000 messages from adolf@hitler.com containing a threat to repeat the Holocaust. The murder of six million more Jews, the sender threatened, would start Nov. 9 - the anniversary of Kristallnacht, the Nov. 9, 1938 'Night of Broken Glass' when the Nazi regime orchestrated attacks on Jews and Jewish businesses across Germany in a harbinger of the Holocaust. German cyber police conceded they were powerless to investigate because the e-mails were sent via a server in the U.S., material that falls outside German laws that make neo-Nazi propaganda a crime. Germany has

repeatedly complained that U.S. free speech laws have crippled its efforts to stop the spread of Neo-Nazi ideas via the Internet. Stalking, harassment, hate-filled and racist speech perpetrated over computer networks may or may not be criminal activities, depending on the jurisdiction."

Germany's Investigating Authority could not do much to help the victims of the threatening email. As it indicated above, the US Free Speech, guaranteed by the First Amendment, was prohibiting the investigation. In this case the USA domestic law did protect the criminal responsible for sending those threatening e-mails.

Goodman and Brenner (2002a) state "that the emergence of cybercrime in its networked and interconnected nature makes it imperative to achieve transnational consistency in criminal prohibitions. One way to accomplish this would be to create a single code of law governing the commission of cybercrime."

The Single Universal law will be the most effective if not the only way to face cybercrimes. Countries need to work together and to cooperate in these issues. As long as some activities are not criminalised in all countries, cyber criminals benefit by not facing the law.

To avoid such a thing of evidential difficulties, the investigation authorities should be equipped with necessary and relevant training in computer and forensic investigation. Lawyers alike should also be trained in computer crime, so that the gap can be minimized. Countries need to cooperate assist each other with investigation of cybercrimes and computer breaches where possible.

6.5 CONCLUSION

A court in Namibia may come to a decision to convict crimes that have effect in Namibia, even the location of the act did not happen within

the Namibia territory. The problem will be on implementation side of such court decision in the foreign states.

More than one country may claim jurisdiction over the action/crimes that was committed over the internet. Recommendation from the Convention on Cybercrime is that the parties claiming jurisdiction should reach agreement between themselves. The agreement will depend whether the political relationship between such countries and their existing domestic law.

Certain activities over the cyberspace must be uniformly regulated as crime in any country. The Convention also makes provision for the extradition, but subject to criminal offences being punishable under the laws of both parties concerned.

According to Magnin (2001)," the Computer Hacking and Intellectual Property section of the U.S. Department of Justice has said, the United States 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 computer-related crimes."

Each country will benefits from ratifying the Convention on Cybercrime yet there is less effort from the member states on effort for most countries to became signatory to Convention.

CHAPTER 7: TAXES IMPLICATION ON E-COMMERCE

7.1 Introduction

The Namibian ECT Bill is silent about tax issues as no provision is made in the ECT Bill. Whether the issue of tax on e-commerce is dealt with by other existing legislation or not, is beyond the scope of this research. The question is that, whether the existing legislation will be sufficient enough to deal with such sophisticated e-commerce transactions on the internet?

Namibia should not be an exemption when it comes to tax on e-commerce, there should a law to govern this. Kerimov (2002) stated that "Tax authorities of all countries found themselves as struggling with the ability to give timely responses to ecommerce challenges that grow at a meteoric speed. Existing legal regulations in many instances are silent as to how to treat new types of electronic commercial activities."

Existing laws may be outdated to be applied to the emerging electronic commerce transactions, for the purpose of collecting tax. Chandra (2005) make it clear that the "Principles of residence and source for taxation cannot be applied with certainty in the seamless, borderless and timeless market place of E-Commerce."

7.1.1 Tax Return E-Fill

In the USA, the tax payers submit their income tax return by means of electronic services. According to the Internal Revenue Service (IRS)'s website, it reported that "this year the agency (nation's tax collection agency and administers the Internal Revenue Code enacted by Congress), received nearly 80 million tax returns through e-file, breaking the record set last year. The 2007 level is up about 9 percent from the 73 million returns filed for the same period last year. Of the 139.3 million

returns filed in 2007, 79.98 million or about 57.4 percent were filed electronically."

The demand to return the income tax return electronically will grow at a fast rate in any country. The table below depicts the growth of income tax returns that were submitted online in the USA. Another question will be when will Namibia will be at this stage? The e-fill of the taxi return will speed up the taxi services in general; therefore the Namibian government needs to implement these services as well.

Year	Returns	Total E-file	Percent E-file
1997	121.5 million	19.2 million	15.8%
1998	123.8 million	24.6 million	19.9%
1999	125.9 million	29.3 million	23.3%
2000	128.4 million	35.4 million	27.6%
2001	131.0 million	40.2 million	30.7%
2002	131.7 million	46.9 million	35.6%
2003	131.6 million	52.9 million	40.2%
2004	132.2 million	61.5 million	46.5%
2005	134.0 million	68.5 million	51.1%
2006	136.1 million	73.3 million	53.8%

Fig: .7.1 The number of e-fill in the USA.

Source: http://www.irs.gov/newsroom/article/0,,id=175470,00.html

According to Thierer and de Rugy (2003) "the sale on the internet have crated problem in terms of tax collection." There is no doubt, e-commerce transactions are being conducted on the internet in Namibia. Payments are done electronically on the internet within Namibia as well. Does the Namibian government have the ability to collect tax on such electronic transactions?

Du Plessis (2004) pointed out that a "fundamental problem posed by e-commerce is the identification of the country or countries that have jurisdiction to tax transaction income." Du Plessis (2004) further state that "the essence of electronic commerce is that transactions are carried out without having any regard to national or geographical borders."

Despite the fact that Namibian ECT Bill's aim is to encourage the use of ICTS, e-government and e-commerce services, there might be some grey areas, therefore a relevant law should be in place first. The Namibian government should speed up the implementation of the ECT so that the e-government services will be available to the public.

Thierer and de Rugy (2003) stated that "the rise of national markets and "remote sellers" (mail order, catalog and e-commerce vendors) have posed a different sort of problem for the tax sale system. Interstate sales create a variety of jurisdictional tax collection problem." Namibia should come up with relevant legislation to tackle tax problems created by e-commerce.

7.1.2 Scam on Taxpayers E-Fill.

Despite the benefits and time saving when submitting your income return electronically, one should be aware of e-mail scam and possible fraud that may be associated with online tax services. The IRS (Internal Revenue Service, the United State Department of Treasury) keeps on warning their clients to be carefully about scam e-mails. The picture below shows how the IRS warns the tax payer about the new e-mail scams.

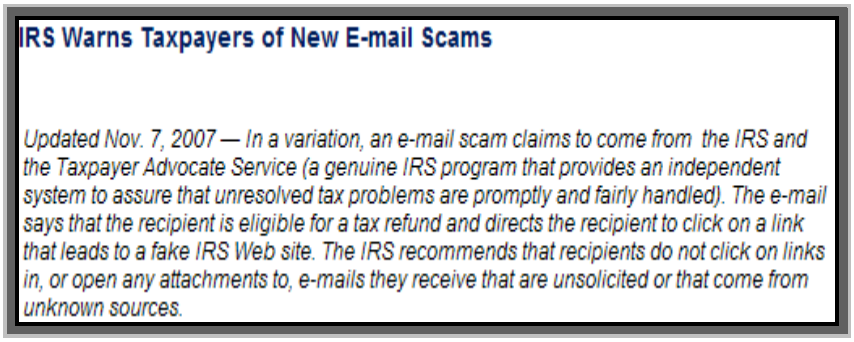


Fig.7.2 a -Warning the taxpayers about phishing mails in the USA.
Source: http://www.irs.gov/newsroom/article/0,,id=170894,00.html

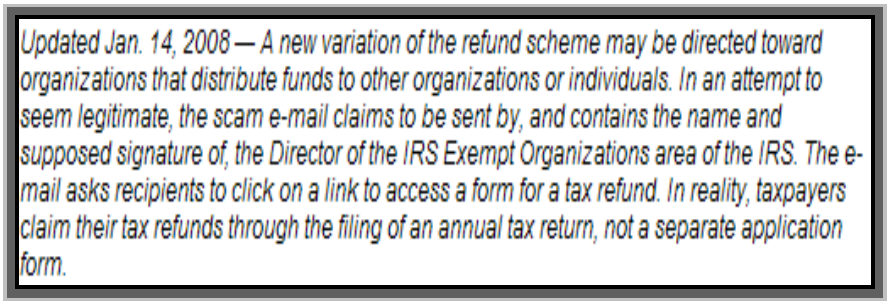


Fig.7.2 b - Warning about phishing mails on tax in the USA.
Source: http://www.irs.gov/newsroom/article/0,,id=170894,00.html

If Namibia comes to a stage where we will be able to submit our tax return electronically, we should be ready to counter such fraudulent scheme. This means that we must have relevant law and legislation in this place regarding this scheme.

ICT security may be the concern in Namibia, considering the necessary skills and knowledge that are required to keep the system security very tight. Ashan (2007) pointed out that "Although US information technology is the most advanced in the world, its information systems have not adequately supported the homeland security mission."

"We are living in a world where most of the information systems must be secure or they will not be used. Consider for instance, the implications of a bank or a healthcare information system without provisions for security" (Mouritidis, 2007). If Namibia intends to have the income tax return submitted online, then the security issue should be dealt with first.

7.2 Existing Law on E-commerce Tax

Existing laws, in any country, are not sufficient enough to deal with issues arising out of ICT and advanced e-commerce. Kerimov (2002) stated that "The rapid growth of electronic commerce has forced governments of many countries to seek appropriate legal policy for its regulation. One of the keenest legal issues related to e-commerce remains to be taxation of revenues generated on the Web. It appeared that current tax laws may

not be capable of addressing the novel issues brought on by e-commerce."

Hellerstein (2000) states that "There must be enough simplification of sales and of taxes uses to make destination-based taxation of sales feasible. Such simplification might include, for example, unification of the tax base across states, unification of tax rates within states, and/or sourcing of sales only to the state level, as well as simplification of administrative procedures."

There might be another law in Namibia which deals with the issues of tax on e-commerce transaction; hence there is no provision of tax on e-commerce in ECT Bill. Thierer and de Rugy (2003), pointed out that "the sale on the internet have crated problem in terms of tax collection." As a result government should come up legislation to deal with sale on the internet. We should learn from the country that had deal with same dilemma; that if there is no other law dealing with the issue of e-commerce, then we should preparing for one as government might revenue from e-commerce.

Wasserman (1998) raised a concern on levying the tax on the e-commerce that "Given the nature of electronic commerce, countries will either have to redefine their permanent establishment thresholds for levying taxes or shift towards a more realistic, residence-based taxing regime. Tax authorities will find it difficult, if not impossible, to administer and police the flow of global electronic commerce."

"While in South Africa there is a provision in the ECT Act as to how deal with taxes on the web based sales. The question is still whether the existing indirect tax principle can be successful applied to the taxation of electronic commerce in a way that will satisfy the competing demand of national revenue collecting agencies". (de Wet and du Plessis 2003, Cyberlaw@SA).

There are different types of electronic commerce transactions, which are done on daily basis in the cyberspace. These types of transaction are done between different stakeholders as it can be seen in the pictures below. All these transactions should be subjected to tax regulation for any government to generate its revenue.

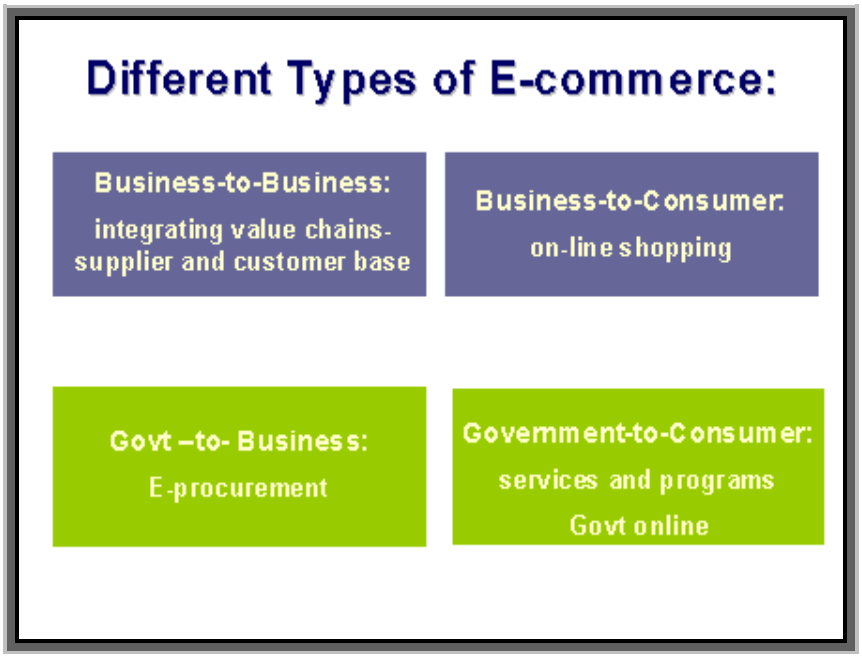


Figure 7.3 Different Types of E-commerce
Source: http://www.taxationweb.co.uk/businesstax/article.php?

7.3 Conclusion

South Africa has identified the ability to income arising from electronic commerce, as one of the reasons to change the tax system from a source based system to a full residence –based system.

Wasserman (1998) concluded that "In order for countries to maintain their tax bases and to avoid double taxation conflicts, the new forms of commerce must be analogized to their functional equivalents in the traditional tax code."

Namibia should come up with law to guide the administration of the tax sales on the internet, if there is no such law in Namibia.

CHAPTER 8: Comparing Namibian ECT Bill with other Cyber Laws

8.1 ECT Laws compared in this Research

Malta ECT Act

Malta's Data Protection Act has a provision that regulating the transfer of personal data to a third country. This provision prohibits the personal data to be transferred to the third country, unless the third country has ensured that there is an adequate level of protection of such data. The Data Protector Commissioner may decide whether the third country ensures an adequate level or not.

In Malta it is illegal for a person to knowingly discloses any password, access code, or any other means of gaining access to any program or data held in any computer system: for any wrongful gain, for any unlawful purpose or knowingly that that it is likely to cause prejudice to any person, such a person shall be liable to a fine not exceeding 50,000.00 rupees and to a term of imprisonment not exceeding 5 years.

Mauritius ECT Act

Mauritius CMC Act makes provision that the Intermediate Court shall have jurisdiction where the act constituting an offence, under this Act (The Computer Misuse and Cybercrime Act 2003) has been committed outside Mauritius -

(a) On board a Mauritian ship; or

(b) On board an aircraft registered in Mauritius.

How is Mauritius going to deal with offence committed from another country and that offence has an effect in Mauritius? Possibility does exist that cybercrime may be committed from anywhere in the world targeting any country and Mauritius will not be an exception.

Goodman and Brenner (2002a), points out that "Cybercriminals can exploit gaps in their own country's criminal law to victimize their fellow citizens with impunity. They can also exploit gaps in the criminal laws of other countries to victimize the citizens of those and other nations; as the "Love Bug" episode demonstrated, cybercrime is global crime."

It is obvious that the cybercriminals are targeting the loophole in any jurisdiction, especially if the specific act/law does not make provision legally with respect to certain issues.

USA ECT ACT

The United States' basic federal computer crimes provision –18 U.S. Code 1030 – allows the U.S. government to exercise jurisdiction over criminal activity that "affects interstate or foreign commerce or communication of the United States."

Tasmania

Likewise, Tasmania claims jurisdiction over cybercrimes, if they have a substantial harmful effect in Tasmania: There is a real and substantial link with Tasmania "where the act or thing was done wholly outside Tasmania or partly within Tasmania, if substantial harmful effects arose in Tasmania."

Mauritius

Section 19 (2) (a) of Mauritius' act stipulate that "The Intermediate Court shall also have jurisdiction where the act constituting an offence under this Act has been committed outside Mauritius

Comparing the provisions in laws above, the Namibian ECT Bill makes provision for a Namibian court to have a jurisdiction over illegal activity that have an effect in Namibia, even though it was committed outside the Namibian borders.

The Mauritius computer act seems to have made similar provision as well but differ slightly from others.

Singapore

Singapore has two acts, i.e. Electronic Transaction Act 54 of 2004, as amended and Computer Misuse Act of 42 of 2005 as amended. In Namibia, the ECT Bill is still to be passed in the parliament, to be becomes an act.

8.2. Recent Development

Sri Lanka has (May 08, 2007 on Tuesday) enacted the Computer Crimes Bill introducing legislation which gives more power to law enforcement agencies when fighting computer crimes, the government ICT agency said.

Olaki (2007) pointed out that The Ugandan Minister of Information and Communication Technology has explained that "Liberalised information can lead to unwanted uses and usage leading to cyber crime. It is necessary to have legal infrastructure within which the technologies can be used. There are three bills which have been drafted, the Electronics Transactions Bill, Digital Signatures Bill and the Computer Misuse Bill,"

Uganda had three bills; all about computer related at a time in comparison with Namibia having only one ECT Bill.

CHAPTER 9: Cybercrime Cases

9.1 Introduction

This chapter discusses some cybercrime cases that were brought before the court. It is important to discuss those cases and to learn from them.

Singh (2005) concluded that "Moreover, international cooperation is increasingly required to successfully resolve crimes, resulting in the need for comprehensive treaties between nations".

To date researches have shown that adequate law should be in place to avoid similar delays in dealing with cybercrime cases, which some countries had experienced. Cybercriminal go unpunished as a result of government not having strong evidence to prove the case against the suspect.

Some countries have either amended their existing cyber crime laws as it can be seen on the figure below.

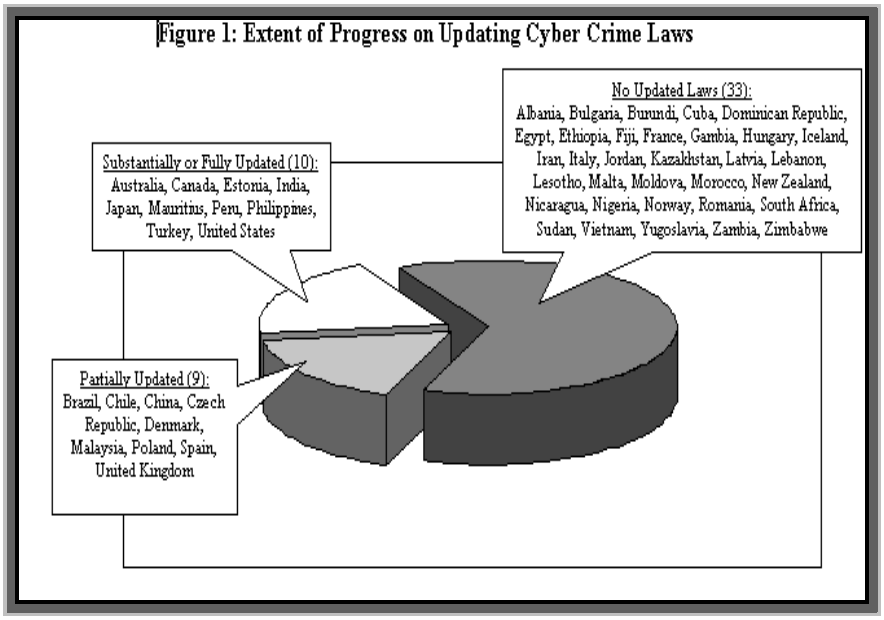


Fig 9.1: Extent of Progress Cyber Crime Laws.
Source: http://www.library.cornell.edu/colldev/mideast/cycrime.pdf

9.1.1 University of Texas

This case of the former **University of Texas** student Christopher Andrew Phillips, who was sentenced to five years of probation and ordered to pay U$170,056 in restitution for hacking into UT's computer system.

This is one the example that for the cases that had been successfully brought before the court and the culprit was convicted. .

9.1.2. Yahoo! Inc Case

"In November 2000 French court gave US-Based Yahoo! Three months to prevent French citizens from accessing similar material, although such publication is allowed under US free speech provisions, the French law does not apply in the US and many experts argue that technology won't permit such differentiation" (Arnold, 2007a). In this case, the French court has taken a decision against the company based in the USA. Despite that a decision was reached and made in the French court there was no means of such decision to be enforced in the foreign country.

Geist (2001) stated that "Since Nazi memorabilia is protected under U.S. free speech laws, the auction were entirely lawful there." This demonstrates that what is legal in Namibia or in any other country does not necessarily mean that it is legal in another country and vice versa.

Reidenberg (2005) stated that "In the now famous French case, the U.S. company transmitted image of Nazi objects that were constitutionally protected in the United States, but illegal to display in France where the users located and where Yahoo! Target advertising."

Solution to such issues is to come up with legal frame work where the single universal law will be applicable to all country connected to the

internet. The dilemma is the differences in culture, tradition, beliefs and religions which vary from one state to another.

The court in one country can comes to a decision, but such country cannot enforce its decision in another jurisdiction (country). "In the United States' federal system, this problem is dealt with by the ``full faith and credit clause'' of the Constitution; each state, in other words, is bound to respect and to enforce judgements duly entered by courts in other States.*13 However, a nation cannot technically enforce its law on a person residing in another country."(Hamano, 2000).

There is an outcry or common understanding; as stated by Rustad and Koenig (2005) that "Global Internet law must develop effective mechanisms to facilitate cross-border enforcement of national judgments." This effort will be achievable if all the countries are cooperating and committed toward that objective.

9.1.3 Lovebug Case

The Love bug case has been highlighted and referred to before, in this research, is one of the good examples that a state may learn a lesson from.

"In May of 2000, the "Love Bug" virus appeared on the Internet and spread around the world in two hours.18 It is estimated to have affected over forty-five million users in over twenty countries, and to have caused between two and ten billion dollars in damage"(Brenner &Koops 2004).

The suspect in this case, cloud not be convicted and the charges against the suspects were dismissed on the grounds that dissemination of virus was not a crime at a time in the Philippines.

9.1.4 DVD Case

According to Stecklow (2005), "Johnasen known as "DVD Jon" writes a program to defeat the geographical-coding restrictions on the DVD player so he could watch American discs -- which cost much less than ones sold in Norway but wouldn't play on European machines. Again he also posted his program on his Web page to share it with others."

This free software can unlock the code and the information on the encrypted DVD movie disk; interested users are able to copy the movie on their pc's hard disk. Kaplan stated that "DVD Jon was tried twice in Oslo in criminal proceedings; he faced maximum punishments of fines and two years in jail, but was acquitted on both times."

Fig: 8. The photo of "DVD Jon"
Source: http://www.nytimes.com/library/tech/00/07/cyber/cyberlaw/21law.html

At the end of the trial the court found that DVD Jon did legally buy the DVDs which he ripped and make a copy for his own. The court did not found any proof that the software, distributed on the internet, was used for illegal purposes.

9.1.5 Jakes Baker's Case

Perritt (1995) stated that "in 1994 a college student named Jakes Baker was prosecuted for communication of threat because he exchanged email message with someone in Canada, elaborating a fantasy of kidnapping and torturing a fellow college student. The charges were dismissed on First Amendment grounds."

The scenario above is one of the issues that existing domestic laws are stumbling block, as far as goal of reaching universal single frame work is concerned.

9.2 CONCLUSION

The cases covered in this chapter had clearly demonstrated that, a lot still need to be done. States need to work together, to overcome the barrier created by different culture, beliefs and by traditional life. Even in states that have the best cyber laws the concern is how to enforcing court decision on other countries.

The Convention on Cybercrime recommends that countries that have ratified the Convention should assist one another in investigation or in prosecutions of the alleged cybercrimes. In absences of assistance and cooperation between the states, the criminals remain free without facing the laws.

Herselman and Warren (2003) concluded that "Governments around the world have recognized the threat of cyber crime and many have been pre-emptive in attempting to bring out legislation protecting against cyber crime. How effective these legislations are…. will still have to be put to the test."

Emphasizing the need to cooperate among states, Calvert (2005a) stated that "A reactive strategy to fighting cyber crime, focusing on law enforcement and investigation after the fact, must be complemented by a strong protective approach through routine, comprehensive

information-sharing and exchange of lessons learned, with the express involvement of the private sector."

CHAPTER 10: RESEARCH METHODOLOGY

10.1 Introduction

This mini-thesis is more a comparative study approach where by the Namibian ECT Bill was assessed and analysed against the similar legislations from other countries. Relevant literatures was analysed and perused to finalize the final stage of this research.

10.2 Objective

The purpose of this research is to highlight the issues concerned with the cybercrimes, computer breaches and cyberspace jurisdiction. Furthermore, the objective is to benchmark the Namibian ECT Bill with enacted ECT Act and cyber laws worldwide.

Similarities and differences on how other ECT Acts has been defined is pointed or highlighted out in this research.

10.3 Data Collection Method

Data were collected mainly from the internet and from the online journals. Books available were used to get information relevant to cybercrimes and jurisdictions.

Academic Research Papers and theses available on the internet have been studied for purpose getting more insight ideas on same topic.

10.4 Research Limitation

There is reasonable number of research papers on the issues of Cybercrimes. Some papers do focus on the specific topic like child

pornography, cyberspace jurisdiction, online contracts, just to mention but a few.

This research's main focus is on the Namibian ECT Bill and Computer breaches in terms of its effectiveness in encountering computer breaches and cybercrimes.

The purpose of this mini-thesis is not to criticise the Namibian ECT Bill in its current format, but rather to assess and compare Namibian ECT Bill with other legislations enacted. Awareness might have been created in some points highlighted. Further, some points highlighted might be used to fill the gap for future researches.

CHAPTER 11: RECOMMENDATIONS AND CONCLUSION

11.1 RECOMMENDATION

In short I have recommended that:

- Namibia needs to secure international cooperation in dealing with cybercrime.
- If possible Namibia needs to ratify the Convention on Cybercrime.
- Namibia has to come up with regulation on technicality of digital signature and on Certification Authority.
- Namibia has to come up with a law on online child pornography.
- If nothing in place so far, Namibia to come up with tax law on e-commerce
- And Namibia needs to speed up the enactment of the ECT Bill.

More details on the above key points are highlighted in the paragraphs below.

Despite that the Namibian ECT Bill is formulated in line with the international and regional inputs, Namibia need to secure cooperation with other states, not only at the regional level but also at the international level when it comes to fighting cybercrimes.

All possible unethical and unacceptable activities in the cyberspace must be uniformly regulated as punishable crime in any given state's law. Similar provisions in cyber laws of states will eliminate possibilities of conflict, disagreement and non-cooperation among countries in the cyberspace.

States worldwide, Namibia Included, should admit that jurisdiction conflict will be there as long as the ECT Act and cyber laws of each state are different from one another. The jurisdiction conflict may be minimized if there is a single universal cyber law which should form part of each state's domestic law.

Each state will benefits from the Convention on Cybercrime, when it became a member and a signatory to the Convention. Member states need to put more effort and attract more states to became signatory to the Convention on Cybercrime. If all states ratify the European

Convention on Cybercrime, (Namibia as well, has not yet done so), the cybercrime suspect will face the wrath on law anywhere in the world irrespective where s/he is residing.

The Namibian government should come up with the strategy and mechanism on how to generate and manage the digital signature, by means of a regulation. This regulation should also make the provision of the Certification Authority, which should be responsible for the management of the digital signature.

The Law Enforcement Authorities should be well equipped with all the necessary skills and knowledge and with appropriate equipment. The skills will help the staff of Law Enforcement Authorities to deal with complex cybercrimes that are on the increase nowadays.

With the absence of appropriate child protection legislation in place, the children in Namibia may be subject to abuse of online pornography. Namibia should come up with the relevant law to regulate child pornography and protect the child from the online pornography and all potential harmful activities against the child, in the cyberspace.

States worldwide needs to cooperate in the combating the tax issues and challenges created by the e-commerce, as transaction may happen between any states worldwide. There is no provision dealing with tax on ecommerce in Namibian Ect Bill. If this is not catered for in another law in Namibia then, then there is a need to formulate one.

States worldwide should adopt a common ground when they outlaw illegal activities, so that cybercrimes are outlawed similar in all states. Electronic transaction and e-commerce transaction in the cyberspace need to be properly regulated, hence a proper cyber legislation should in place in Namibia, the sooner the better.

11.2 CONCLUSION

In summary I have also concluded that:

- Existing laws are not adequate to regulate cybercrimes.
- Internet users are vulnerable in the absence of cyber laws in place.
- Namibia ECT Bill is in line with recent international development on cyber law.
- No country alone can fight cybercrime without assistance of the other.
- With differences in national cyber laws, jurisdiction conflict is here to stay.
- Countries will benefit when ratify and become a member to the Convention on Cybercrime.

More information about the points above is in the following paragraphs below.

The information and communication technology revolution has challenged the existing law in any given states. The existing domestic laws are no longer adequate to regulate illegal and unethical activities over the cyberspace

Uses of computers today have increased, the world has become just a small village and this may expose computer and internet users to the vulnerability attacks by the cybercriminals in the absence of relevant law in place. Internet users need to be protected from such vulnerabilities and other attacks in the cyberspace.

Cybercrime is one of the top priority crimes on the Interpol's list; therefore it is a necessity for Namibia to have relevant law on cybercrimes. Comparing the Namibian ECT Bill with other Cyber laws worldwide, the Namibian ECT Bill is on par with the recent development on the cybercrimes. The Namibian ECT Bill once enacted will be effective in prevention and in regulation of the cybercrimes, as most of the cybercrimes are provided for in the ECT Bill.

In general, provisions in the Namibian ECT Bill on cybercrimes are in line with what are provided for in the European Convention on

Cybercrimes. States like Norway and Philippine have paid a price of not having adequate and proper legislation with regards to cybercrimes. Therefore the process to make the Namibia ECT Bill an act should be sped up, for Namibia not to suffer same consequences as other countries did.

With inputs from the UNITRAL Model Law and the SADC Model Law on Electronic Commerce and Transactions, the Namibian ECT Bill is crafted very well, in an attempt to prevent cybercrimes.

In the Namibian ECT Bill there is a provision for the contract to be concluded and signed online, so there is no need for parties to have physical meeting. The legal recognition of the data message, acceptance of contract online and evidential weight and admissibility of the data message in the court will make our life easier. All of these are provided for in the Namibian ECT Bill.

Namibia as country will not successfully defend itself from the threat of cyber criminals alone; we will still need help from other countries. This need effort and involvement of all stakeholders in the cyberspace. At this point in time every state criminalize what it feel is necessary to, hence given such differences in national laws worldwide.

Cyber jurisdiction will be a challenge as long as each state has its cyber law different from another state. The fact remain that every cyber law is based on countries' physical boundaries, while internet is not limited to any geographical boundary at all. The issues of childhood age limit might be open to potential child abuse as age limit is defined differently from state to state. The people with ill intention might target those states where age limit is low, so that they may fulfil their ill intention without facing the law.

States will benefits from the Convention on Cybercrime, when they become signatory, regrettably there is less effort on the member states to secure more signatories to Convention on Cybercrime.

The cybercrime cases covered in chapter 9 in this research, had clearly demonstrated to the cyberspace world, that, a lot still need to be done. For a state tries to implement its court decision in another foreign state had proven to be futile.

In the absences of assistance and cooperation between the states at regional and international level, the cyber criminal will not face the law, despite having committed punishable cybercrimes. The issue of cyberspace jurisdiction is not unique to Namibia alone, but to the rest of the world at this point in time.

12. Exclusion to ECT Bill

However there are areas where the Namibian ECT Bill, will not be applicable once enacted as an Act of parliament. The ECT Bill has the exemption that it will not be applicable to the:

- Alienation of Land Act 68 0f 1981
- Wills Act 7 of 1953
- Bills of Exchanges Act 34 of 1964
- Stamp Duties Act 77 of 1968
- A sales contract for the alienation of immovable property;
- A long term lease (longer than 10 years) of immovable property
- A will; and
- A cheque or bill of exchange.

13. REFERENCES:

1. Goodman, M. D. and Brenner, S. W. (2002a) "Cybercrime the need to harmonize the National Penal and Procedural Laws," Accessed on 17th March 2007, from http://www.isrcl.org/Papers/Brenner.pdf

2. Goodman, M. D. and Brenner, S. W. (2002b). "The Emerging Consensus on Criminal Conduct in Cyberspace" accessed from http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php#FN_35 UCLA Journal of Law and Technology.

3. Brenner, S. W. and Koops, B. (2004). "Approaches to Cybercrime Jurisdiction" . Journal of High Technology Law, Vol. 4, No. 1, 2004 Available at SSRN: http://ssrn.com/abstract=786507

4. Koops, .B. (2005). "Cybercrime Legislation in the Netherlands" . Cybercrime and Security, Vol. 2005/4, pp. 1-20, 2005 Available at SSRN: http://ssrn.com/abstract=918757

5. Koops, B. (2003). "The Shifting 'Balance' Between Criminal Investigation and Privacy. A Case Study of Communications Interception Law in the Netherlands" . Information, Communication & Society, Vol. 6, No. 3, pp. 380-403, 2003 Available at SSRN: http://ssrn.com/abstract=786524

6. Brenner, S. W. and Clarke, L. L.(2005). "Should Commercial Misuse of Private Data be a Crime?" (November 1, 2005). Available at SSRN: http://ssrn.com/abstract=845845

7. Brenner, S. W. (2002). "Organized Cybercrime? How Cyberspace May Affect The Structure of Criminal Relationships" North Carolina Journal of Law & Technology Vol. 4 No.1 2002. Accessed on 7th April 2008, Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=436280

8. McConnell International LLC (2000) "Cyber Crime and Punishment?" Archaic Laws Threaten Global Information December 2000, Accessed 14th March 2007 from http://www.library.cornell.edu/colldev/mideast/cycrime.pdf

9. Cox, N. (2006)." "Cyber-crime Jurisdiction in New Zealand", in Bert-Jaap Koops, Susan Brenner, Paul de Hert (eds), Cyber-crime Jurisdiction: A Global Survey (T.M.C. Asser Press, The Hague, 2006) 177-188" Accessed on 17th March 2007 from http://www.geocities.com/noelcoxfiles/Cyber-Crime.pdf

10. Grabosky, P (2000a). "Cyber Crime and Information Warfare" Accessed on 17th March 2007 from http://www.aic.gov.au/conferences/transnational/grabosky.pdf

11. Grabosky, P, (2000b). Computer Crime in a World Without Borders, Retrieved on 15th November 2007, Retrieved from http://www.afp.gov.au/about/publications/platypus_magazine/june_2000/compcri

12. Arnold, B. (2007a). "Caslon Analytics guide cyberspace governance" Accessed on 17th March 2007, Retrieved from http://www.caslon.com.au/governanceguide4.htm

13. Arnold, B. (2007b). "Caslon Analytics e-politics guide" Accessed on 17th March 2007, Retrieved from http://www.caslon.com.au/politicsguide6.htm

14. Mills K. (2003). "Effective Formation of Contracts by Electronic Means: Do We Need a Uniform Regulatory Regime?", Accessed on 17th March 2007 from http://www.karimsyah.com/imagescontent/article/20050922170958.pdf

15. Calvert, W. J. (2005a). "Council of Europe Convention on Cybercrime: Themes and Critiques" Accessed on for http://www.netdialogue.org/discussion/?p=22

16. Calvert, W. J. (2005b). "Trends in International Cyber Crime and Public-Private Countermeasures", Accessed on 29th May 2005, from http://www.ischool.berkeley.edu/~cjones/Full%20Text%20Papers/Trends%20in%20International%20Cyber%20Crime%20and%20Public-Private%20Countermeasures.pdf

17. Argy, P. and Martins, N. (2001). "The effective formation of contracts by electronic means" Retrieved on 12th May 2007, from http://www.nswscl.org.au/journal/46/Argy.html

18. BABU, M. (2004). "WHAT IS CYBERCRIME?" ACCESSED ON 12TH MAY 2007 FROM http://www.crime-research.org/analytics/702/

19. Paul, B. (2001). "The write staff? Recent Developments in electronic signatures" Retrieved on 12th May 2007, Accessed from http://www.nswscl.org.au/journal/46/Barnett.html#FN*

20. Carey, T. C. (2000), "Jurisdiction and Contract Formation" Retrieved on 19th May 2007, from http://www.bromsun.com/media/contract_issues.pdf

21. Putnam, L. D. & Elliot, D. D. (2001). "International Responses to cyber crime," Retrieved on 27th May 2007 from http://media.hoover.org/documents/0817999825_35.pdf

22. Archick, K. (2004). "CRS Report for Congress, Cybercrime: The Council of Europe Convention" Retrieved on 27th June 2007, from http://fpc.state.gov/documents/organization/36076.pdf

23. Austin Business Journal Sept. 2006 "UT hacker gets five years' probation" accessed 2nd August 2007, retrieved from http://austin.bizjournals.com/austin/stories/2005/09/05/daily12.html

24. MacDonnell, H. (2007). "Scotland to raise age limit for buying cigarettes to eighteen" Retrieved on 10th July 2007, Accessed from http://news.scotsman.com/topics.cfm?tid=663&id=875692007

25. KAPLAN, S. C. (2000). "Norwegian Teenager Appears at Hacker Trial He Sparked" Retrieved on 13th August 2007 from http://www.nytimes.com/library/tech/00/07/cyber/cyberlaw/21law.html

26. Stecklow, S. (2005). "Meet the 21-yr-old Norwegian who defied Hollywood" Retrieved on 13th August 2007 from http://www.post-gazette.com/pg/05290/590139.stm

27. Allen, E. (2006). "Child Pornography: Model Legislation & Global Review" Accessed on 13th August 2007 from http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf

28. Kolsrud, K.(2003). "DVD Jon' scores huge legal victory" Retrieved on 26th September 2007 accessed from http://www.aftenposten.no/english/local/article466519.ece

29. Wotley, R. & Smallbone, S. (2006). "Child pornography on the internet" Retrieved on 12th September 2007, accessed from http://www.cops.usdoj.gov/mime/open.pdf?Item=1729

30. Nemerofsky, J. (2000). The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of It?, 6 RICH. J.L. & TECH. 23 (Spring 2000) http://law.richmond.edu/jolt/v6i5/article2.html

31. Kowalski, M. (2002). "Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics" Accessed on 14th November 2007,

Retrieved from http://dsp-psd.pwgsc.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf

32. Olaki, E. (2007). Uganda: New Cyber Laws Offing Accessed on 11th September 2007, from http://allafrica.com/stories/200707040150.html

33. (2007). "Certification Authority" Retrieved from http://www.webopedia.com/TERM/C/certification_authority.html Accessed on 27th September 2007.

34. Chandra, N. (2005). "Issues, Approaches and Solutions in Taxation of Electronic Commerce – Taxation Web" Accessed on 22nd October 2007 from http://www.taxationweb.co.uk/businesstax/article.php?id=191

35. McIntyre, T. J. (2005) Computer Crime in Ireland: A critical assessment of the substantive law, Accessed on 15th November 2007, Retrieved from http://www.tjmcintyre.com/resources/computer_crime.pdf

36. Kerimov, N. G. (2002). Current Problems of International Taxation of Electronic Commerce" Accessed on 22nd October 2007 Retrieved from http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1023&context=stu_llm

37. Levine, R. (2006). "Unlocking the iPod" Retrieved on 13th August 2007, from http://money.cnn.com/magazines/fortune/fortune_archive/2006/10/30/8391726/index.htm

38. Christensen, S. (2001). "Formation of Contract by Email – Is just the same as the Post?" Accessed on 29th October 2007, Retrieved on from http://www.law.qut.edu.au/ljj/editions/v1n1/pdf/s_christ.pdf

39. Swanson, J. (2002). "Vandals at the gates"- Comment on Internet and Network Security and the Law in Canada, Accessed on 30th October 2007,

Retrieved from http://www.e-future.ca/sask/ebusiness/vandals_at_the_gates.pdf

40. Thierer, A.D. and de Rugy, V. (2003) "The Internet Tax Solution Tax Competition, Not Tax Collusion. Accessed on 1st November 2007, Retrieved from http://www.cato.org/pubs/pas/pa494.pdf

41. Kende, M. S. (1997). "The Impact of Cyberspace on the First Amendment" Retrieved on 13th November 2000, Accessed from http://www.vjolt.net/vol1/issue/vol1_art7.html

42. Magnin, C. J. (2001). "The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?" Accessed on , Retrieved from http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf

43. Burk, D. L. (1997). "Jurisdiction in the world without borders" VIRGINIA JOURNAL *of* LAW *and* TECHNOLOGY Accessed from http://vjolt.student.virginia.edu/graphics/vol1/vol1_art3.html#Introduction#Introduction

44. Kondo, L. L. (2002). Untangling The Tangled Web: Federal Court Reform Through Specialization For Internet law And Other High Technology Cases" Retrieved on 5th November 2007, Accessed from http://www.lawtechjournal.com/articles/2002/01_020309_kondo.php

45. Hong, H. (1998). "Hacking Through the computer Fraud and Abuse Act" Retrieved on 5th November 2007, Accessed from http://www.lawtechjournal.com/archives/blt/i3-hh.html

46. Wasserman, R. (1998). "International tax Consequences of Electronic Commerce." Retrieved on 5th November 2007, Accessed from http://www.lawtechjournal.com/archives/blt/i3-rw.html

47. Hamano, M. (2000). "Chapter T. The Principles of Jurisdiction: Comparative Study in the Approach to Jurisdiction in Cyberspace" Access on 22nd May 2007, Retrieved for http://www.geocities.com/SiliconValley/Bay/6201/
48. Herselman, M. & Warren M.(2003) "Cyber Crime Influencing Businesses in South Africa" Accessed on 13th November 2007, Retrieved from http://proceedings.informingscience.org/InSITE2004/045herse.pdf

49. Burke, L. (2000). "Love Bug Case Dead in Manila" Accessed on 12th November 2007, Retrieved from http://www.wired.com/print/politics/law/news/2000/08/38342

50. Magele, T. (2005). "E-Security in South Africa" Accessed on 12th November 2007, Retrieved from http://www.sabinet.co.za/images/ejour/ju_sajcj/ju_sajcj_v19_n3_a1.pdf

51. Alaganandam, H., Mittal, P., Singh, A. & Fleizach, C. (2005). " Cybercriminal Activity" Accessed on 14th November 2007, Retrieved from http://sysnet.ucsd.edu/~cfleizac/WhiteTeam-CyberCrime.pdf

52. Reidenberg, J R. (2005). "Technology and Internet Jurisdiction" . University of Pennsylvania Law Review, Vol. 153, p. 1951, 2005 Available at SSRN: http://ssrn.com/abstract=691501

53. Reidenberg, J. R. (2001). "The Yahoo Case and the International Democratization of the Internet" (April 2001). Fordham Law & Economics Research Paper No. 11. Available at SSRN: http://ssrn.com/abstract=267148 or DOI: 10.2139/ssrn.267148

54. Michael, G. (2001). "IS THERE A THERE THERE? TOWARD GREATER CERTAINTY FOR INTERNET JURISDICTION" Accessed on 14th November 2007, Retrieved from http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf

55. Perritt, H. H. (1995). "Computer Crimes and Torts in the Global Information Infrastructure: Intermediaries and Jurisdiction." Accessed on 14th November 2007, Retrieved from http://www.kentlaw.edu/cyberlaw/resources/interjuris.html

56. Bosen, B. (2006). "Network Attacks: Analysis of Department of Justice Prosecution." 1999-2006. Retrieved on 14th November 2007. Accessed from https://forms.phoenix.com/cybercrime/docs/cyberdoc.pdf

57. Geist, M. (2001). IS THERE A THERE THERE? TOWARD GREAT CERTAINTY FOR INTERNET JURISDICTION." Accessed on 14th November 2007. Retrieved from http://arxiv.org/ftp/cs/papers/0109/0109012.pdf

58. Coombs, D. (2006) Non-Repudiation, A Fingerpuppet-Theatre Guide" Accessed on 27th April 2007, Retrieved from http://www.carillon.ca/library/nonrepudiation_1.2.pdf

59. Hellerstein, W. (2000). "DECONSTRUCTING THE DEBATE OVER STATE TAXATION OF ELECTRONIC COMMERCE." Accessed on 15th November 2007 Retrieved from http://jolt.law.harvard.edu/articles/pdf/v13/13HarvJLTech549.pdf

60. Mann C. L. (2000). "TRANSATLANTIC ISSUES IN ELECTRONIC COMMERCE." Retrieved on 15th November 2007, Accessed from http://www.iie.com/publications/wp/00-7.pdf

61. Jones, R. & Basu, S. (2001). Taxation of Electronic Commerce: A Developing Problem. Accessed on 15th November 2007, Retrieved from http://www.bileta.ac.uk/01papers/rjones.html

62. Rustad, M. L & Koenig, T. H. (2005) "Harmonizing Cybertort Law for Europe and America", Accessed on 22nd November 2007, Retrieved from

http://www.law.suffolk.edu/faculty/addinfo/rustad/HarmonizingCybertortLaw.pdf

63. Petropoulos, D & Kotzanikolaou, P. () "A framework for transaction non-repudiation demonstrable log completeness" Accessed on 13th March 2008, Retrieved from http://www.encodegroup.com/pdf/esp0402.pdf

64. McCullagh A. & Caelli, W. (2000) " Non-Repudiation in the Digital Environment" Accessed on 13th March 2008, Retrieved from http://www.firstmonday.org/issues/issue5_8/mccullagh/

65. Watney M. (2007a) "State surveillance of the internet: human rights infringement or e-security mechanism? *Int J. of Electronic Security and Digital Forensics,* Vol. 1, No,1, pp42-54. Accessed on 9th April 2008, Retrieved from http://www.inderscience.com/storage/f126425971011183.pdf

66. Watney M. (2007b) "The evolution of legal regulation of the internet to address terrorism and other crimes" Accessed on 14th April 2008. Retrieved from http://search.sabinet.co.za/images/ejour/ju_tsar/ju_tsar_2007_n3_a4.pdf

67. Watney M.(2005). "REGULATION OF INTERNET PORNOGRAPHY IN SOUTH AFRICA" Accessed on 9th April 2008, Retrieved from http://www.isrcl.org/Papers/2005/Watney.pdf

68. Jahankhani , H. (2007) "Evaluation of cyber legislations: trading in the global cyber village" *Int J. of Electronic Security and Digital Forensics,* Vol. 1, No,1, pp1-11. Accessed on 9th April 2008, Retrieved from http://www.inderscience.com/storage/f128591174321610.pdf

69. Mouratidis, H (2007) "Secure information systems engineering: a manifesto" *Int J. of Electronic Security and Digital Forensics,* Vol. 1, No,1, pp27-41. Accessed on 9th April 2008, Retrieved from http://www.inderscience.com/storage/f825109126117143.pdf

70. Angelopoulou, O. Thomas, P., Xynos, K. and Tryfonas T.,(2007) "Online ID theft techniques, investigation and response" *Int J. of Electronic Security and Digital Forensics,* Vol. 1, No,1, pp76-88. Accessed on 9th April 2008, Retrieved from http://www.inderscience.com/storage/f361141587291210.pdf

71. Ahsan S.(2007) "IT enabled counter terrorism infrastructure: issues

and challenges" Retrieved on 9th April 2008, Accessed from http://www.inderscience.com/storage/f537111126948210.pdf

72. Li, X. (2007) 'International Action against Cybercrime: Networking Legal Systems in the Networked Crime Scene" Retrieved on 7th May 2008, accessed from http://www.webology.ir/2007/v4n3/a45.html

73. Chawki, M (2005) "A critical look at the Regulation of Cybercrime " A Comparative Analysis with Suggestion for Legal Policy: Accessed on 4th April 2008, Retrieved from http://www.crime-research.org/library/Critical.doc

74. Nel, S. (2004) "*Freedom of expression and the Internet*" in Buys (ed) *Cyberlaw@SA II* (2004) 216.

14. Bibliography

1. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm
2. http://www.irs.gov/newsroom/article/0,,id=175470,00.html
3. http://www.treasury.gov.au/contentitem.asp?NavId=014&ContentID=1083
4. http://www.weblaw.edu.au/weblaw/display_page.phtml?WebLaw_Page=e-Commerce+Law
5. http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf
6. http://www.cybercrime.gov/COEFAQs.htm#Q4
7. http://www.parliament.gov.na/parliament/billsandacts/Actsonfp.asp
8. http://www.lawtechjournal.com/archives.php
9. http://www.lawtechjournal.com/articles/2002/01_020309_kondo.php
10. http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php
11. http://www.ic3.gov/crimeschemes.aspx
12. http://www.geocities.com/noelcoxfiles/Cyber-Crime.pdf
13. http://www.caslon.com.au/governanceguide4.htm
14. http://www.aic.gov.au/conferences/transnational/grabosky.pdf
15. http://www.karimsyah.com/imagescontent/article/20050922170958.pdf
16. http://www.isrcl.org/Papers/Brenner.pdf
17. http://www.law.qut.edu.au/about/ljj/editions/v1n1/pdf/s_christ.pdf
18. http://www.bromsun.com/media/contract_issues.pdf
19. http://www.jurisdiction.com/ecom3.htm
20. http://www.interpol.int/
21. http://www.securityhorizon.com/journal.php
22. http://media.hoover.org/documents/0817999825_35.pdf
23. www.opm.gov.na/elaws/downloads

24. http://www.bu.edu/law/scitech/volume1/KAIN.PDF#search=%22Journal%20of%20Computer%20Breaches%20and%20conviction%22
25. http://www.journalonline.co.uk/article/1001709.aspx
26. http://law.richmond.edu/jolt/v6i5/article2.html
27. http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,71972,00.html
28. http://austin.bizjournals.com/austin/stories/2005/09/05/daily12.html
29. www.mcconnellinternational.com
30. www.coe.int
31. http://www2.warwick.ac.uk/fac/soc/law/elj/jilt
32. http://www.naavi.org/pati/pati_cybercrimes_dec03.htm
33. http://www.infragard.net/press_room/articles/article_030305.htm
34. http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php
35. http://lawprofessors.typepad.com/whitecollarcrime_blog/computer_crime/index.html
36. http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf
37. http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume122/documents/Pastukhov_WEB_000.pdf
38. http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=2337
39. http://www.missingkids.com/en_US/documents/CP_Legislation_Report.pdf
40. http://www.missingkids.com/en_US/documents/CP_Legislation_ExecutiveSummary.pdf
41. http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2336
42. http://www.mcconnellinternational.com/services/cybercrime.htm
43. http://www.nytimes.com/library/tech/reference/indexcyberlaw.html
44. http://etd.unisa.ac.za/ETD-db/theses/available/etd-08172005-103637/unrestricted/08chapter8.pdf
45. http://www.cops.usdoj.gov/mime/open.pdf?Item=1729

46. http://en.wikipedia.org/wiki/Jon_Johansen

47. http://www.nid.org.na/pub_docs/NID.pdf

48. http://www.phillipsnizer.com/library/caseupdates.cfm

49http://www.wisc.edu/writetest/Handbook/DocAPACitations_Place.html

50. http://owl.english.purdue.edu/owl/resource/540/01/

51. http://www.e-future.ca/sask/ebusiness/vandals_at_the_gates.pdf

52. http://www.jltp.uiuc.edu/archives/Colby.pdf

53. http://press.coe.int/cp/2001/456a(2001).htm]

54. http://www.cato.org/pubs/pas/pa494.pdf

55. http://www.house.leg.state.mn.us/hrd/pubs/inttax.pdf

56. http://www.magnin.org/Publications/home.htm

57. http://lawspace.law.uct.ac.za:8080/dspace/bitstream/2165/323/1/MLHMAM002.pdf

58. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf

59. http://cybercrime.advancedstudies.org/

60. https://forms.phoenix.com/cybercrime/docs/cyberdoc.pdf

61. http://sysnet.ucsd.edu/~cfleizac/WhiteTeam-CyberCrime.pdf

62. http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf

63. http://vjolt.student.virginia.edu/url_errata.html

64. http://web.ncf.ca/at571/compcrime.html

75. http://www.ulcc.ca/en/cls/internet-jurisdiction.pdf

76. http://www.taxationweb.co.uk/businesstax/

77. http://almanhack.com/Information%20Warfare%20-%20Is%20cyberterrorism%20a%20real%20threat.pdf

78. http://jolt.law.harvard.edu/articles/pdf/v13/13HarvJLTech653.pdf
79. http://legis.state.nm.us/LCS/bluetaxdocs/EadsECommerceBRTCTestimonyMay222003.pdf
80. http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/
81. http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/CsaGermany.pdf
82. http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/csaDenmark.pdf
83. http://www.answers.com/topic/non-repudiation?cat=technology
84. http://answers.yahoo.com/question/index?qid=20071224000659AA75k5u
85. http://www.inderscience.com/storage/f126425971011183.pdf
86. http://www.isrcl.org/Papers/2005/Watney.pdf
87. http://search.sabinet.co.za/images/ejour/ju_tsar/ju_tsar_2007_n3_a4.pdf
88. http://www.iwar.org.uk/ecoespionage/resources/cc-issues/ocp32.doc
89. http://www.crime-research.org/library/Critical.doc
90. http://www.oecd.org/dataoecd/29/12/35670414.pdf
91. http://www.webology.ir/2007/v4n3/a45.html
92. http://www.net-security.org/article.php?id=886
93. http://www.treatywatch.org/about.html
94. http://etd.unisa.ac.za/ETD-db/theses/available/etd-08172005-103637/unrestricted/08chapter8.pdf
95. http://www.popcenter.org/problems/child_pornography/
96. http://www.cyber-rights.org/documents/yahoo_ya.pdf
97. http://www.aph.gov.au/Senate/committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf
98. http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf
99. http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf
100. http://www.un.or.at.uncitral
101. http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm
102. http://en.wikipedia.org/wiki/Convention_on_Cybercrime

103. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
104. http://www.usdoj.gov/criminal/cybercrime/senateCoe.pdf
105. http://conventions.coe.int/Treaty/EN/Treaties/Html/189.htm

15. ABBREVIATIONS

ECT Bill –	Electronic Communication and Transaction Bill
EISMC:	Electronic Information Systems Management Council
UNICTRAL –	United Nations Commission on International Trade Law
OECD -	Organisation for Economic Co-operation and Development
MLesig -	Model Law on Electronic Signatures
UCITA -	The Uniform Computer Information Transactions Act
UT -	University of Texas
USA -	United States of America
ICT -	Information Communication & Technology
IRS -	Internal Revenue Services, Department of Treasury (USA)
ECT Act –	Electronic Communication and Transaction Act
CSI –	Computer Security Institute
CoE -	Council of Europe Convention on Cyber-crime
CMC Act –	Computer Misuse and Cybercrime Act of Mauritius