CYBERCRIME: AN ANALYSIS OF CURRENT LEGISLATION IN SOUTH AFRICA

By

Charlotte Beverly Schultz

Submitted in partial fulfilment of the requirements for the degree LLM (Mercantile Law)

Faculty of Law
University of Pretoria

Supervisor: S Papadopoulos

October 2016

DECLARATION

I declare that this mini-dissertation, which I hereby submit to the Faculty of Law, University of Pretoria, is my own work and has not previously been submitted for a degree at any other university. Acknowledgements and references have been provided in accordance with the University's requirements.

ACKNOWLEDGEMENTS

I would like to express my gratitude to my Family and Friends who have shown me unconditional love and support throughout the research of this dissertation. I would not have completed this dissertation without their constant encouragement and prayers.

I would like to thank my supervisor, Sylvia Papadopoulos, for her guidance and advice throughout this dissertation.

I would like to express my gratitude to Sizwe Snail for his guidance and interest in my topic.

KEY WORDS

Cybercrime, cybercriminals, cybersecurity, common law, computer abuse, computer crimes, conventions, harmonise, illegal access, internet crime, jurisdiction, legislation, penalties, legislative shortcomings, the Electronic Communications and Transactions Act, the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), the Cybercrimes and Cybersecurity and Related Matters Bill.

Table of Contents

Chapter 1: Background

1.1 Introduction

With the advent of new technology, new types of crime have surfaced and traditional crimes such as fraud are now being perpetrated by means of sophisticated technology.[1] Traditional boundaries have fallen away and a virtual borderless world has become a platform for crime.[2] From this virtual reality world derives constraints for the traditional methods of detection, investigation and prosecution of crimes which are somewhat constrained in the light of new and advanced cybercrimes.[3]

The purpose of this mini-dissertation is to firstly examine the development of the South African law with the focus on cybercrimes; the criminality of cybercrimes and issues pertaining to the definitions as well as to analyse the effectiveness of the current legislation in addressing this type of crime. A secondary aspect of the paper is an analysis of the Proposed Cybercrime and Cybersecurity and Related Matters Bill[4] (the Bill) and how the Bill addresses current legislation shortcomings.

This dissertation seeks to analyse the development of the South African law and particularly with regards to cybercrimes, including issues relating to the definitions of cybercrime. Furthermore it distils the current legal position and lastly how the above mentioned Bill addresses further shortcomings in our current legal framework.

1.2 Problem Statement and Research Question

Over the last decade great strides have been made in the South African legislation to address issues of cybercrime, from the common law to the promulgation of the Regulation of Interception of Communications and Provision of Communications- Related Information Act (RICA),[5] to the Electronic Communications and Transactions (ECT) Act[6] and now the Bill on Cybercrimes, namely the ECT Act.[7] The most recent development is the Bill on Cybercrimes

1 Unpublished: S. Maat, 'Cybercrime: a comparative law analysis', unpublished LLM dissertation, University of South Africa (2009) 3.

2 *Ibid.*

3 *Ibid.*

4 Published in Government Gazette, volume 603, 2 September 2015, number 39161.

5 Act 70 of 2002, herein after referred to as 'RICA'.

6 Act 25 of 2002, herein after referred to as the 'ECT Act'.

7 F. Cassim 'Formulating specialised legislation to address the growing spectre of cybercrimes: a comparative study' (2009)12 *Potchefstroom Electronic Law Journal* 59.

which was published in the Government Gazette for public commentary which attempts to address the ECT Act's identified shortcomings.

1.3 Overview

During the research process, it became evident that there is no clear recognised definition for the term cybercrime. One of the earliest definitions is given by Parker, who uses the term 'computer abuse' and defines it as: *'Any incident involving an intentional act where a victim suffered or could have suffered a loss, and a perpetrator made a gain and is associated with computers'.*[8]

Building on this definition, Casey[9] has drawn out four distinct elements which Parker's definition presents, namely; (1) the computer being the target of the crime, (2) the computer being used as an instrument of the crime, (3) the computer being incidental to the crime and (4) crimes which are associated with the popularity and demand of computers.

Leslie[10] offers the following succinct yet clear definition of cybercrime: *'Cyber Crime is an act that is punishable by law, using an automatic electronic device that performs mathematical or logical functions.'*[11] Leslie's definition still has limitations in that it doesn't provide a clear definition. This definition makes reference to the act which needs to be completed in order for the crime to take place as well as the way in which the crime must be carried out.

According to Cassim[12] cybercrime is a crime which is primarily carried out by means and use of a computer on the internet and thus the computer may be the subject or object of the crime.[13] Cassim describes the objective perspective as the computer being the object for the crime to be carried out when there is theft of software and hardware. The subjective perspective is described as the computer being used as an instrument to commit traditional crimes such as fraud, extortion or 'new' types of cybercrimes such as hacking, unauthorised access to information or the interception of information and cyber terrorism.[14]

Cyber terrorism is an example of a 'new' type of crime which has been brought about by technological advancements. This is a result from the convergence of the physical and virtual

8 D. 'Leslie '*Legal principles for combatting cyber laundering'*, (2014) 27.

9 E. Casey '*Digital evidence and computer crime: forensic science, computers and the internet'* (2004)14.

10 D. 'Leslie 'Legal principles for combatting cyber laundering', (2014) 27.

11 Casey (2004) 19.

12 *Ibid.*

13 Leslie (2014) 27.

14 *Ibid.*

worlds.[15] Cyber terrorism has been defined as a: *'Premeditated use of disruptive activities, or threat thereof in cyber space with the intention of furthering social ideological, religious, political or similar objectives or to intimidate any person in the furtherance of such objectives.'*[16] Cyber terrorist attacks can take different forms such as; a terrorist breaking into a company's computer network causing havoc and sabotaging a company's gas lines or wreak havoc on the international finance system.[17]

Cyber terrorism can be divided into various categories, namely; 'effects based cyber terrorism' which concentrates on the effects of cyber terrorism and 'intent based cyber terrorism' which refers more to the use of the cyber system to plan and execute an act of terror and recruitment and proliferation of terrorist material on email and social media.[18] The above mentioned is a clear demonstration that cybercrime is no longer restricted to computers and the focus has moved to data and information technology.

According to Maat, the first leg of the definition for cybercrime should entail criminalising unauthorised access, and consideration should be given to criminalising the possessions and dealing in devices used to commit the offences. This then allows the first leg of the definition to accommodate the new types of crimes that have emerged with the development of computer and information technology.[19]

Maat[20] goes further by saying that computer extortion, computer related fraud and theft of information, and credit data should fall within the second leg of the definition.[21] Computers and information technology play an active role in the commission of these offences,[22] therefore enabling traditional types of crimes such as extortion or fraud which have existed for ages to be perpetrated by means of sophisticated technology. Maat is therefore of the opinion that cybercrime can be defined as follows: *'Cybercrime encompasses all illegal activities where the computer, computer system, information network, or data is the target of the crime and those known illegal activities or crimes that are actively committed through or with the aid of computers, computer systems, information networks or data.'*[23] Further to this, Maat states

15 Cassim (2009) 36.

16 F. Cassim 'Addressing the spectre of terrorism: a comparative perspective' (2012) 15 *Potchefstroom Electronic Law Journal* 381.

17 Cassim (2012) 381-382.

18 S. Snail 'Cybercrime and Cybersecurity legislation in Africa- with an emphasis on Cyber Terrorism and Cyber Warfare from a South African perspective.'- Document presented at the *Lex Informatica* 8 July 2016.

19 Maat (2004) 21.

20 *Ibid.*

21 *Ibid.*

22 *Ibid.*

23 Maat (2004) 22.

that cybercrime is of a borderless nature and conventional boundaries are no longer the norm.[24]

With reference to the Council of Europe Convention on Cybercrime[25] (Budapest Convention), particularly Article one, the Budapest Convention does not provide for a definition of cybercrime. The Budapest Convention goes as far as defining a 'computer system'[26] and 'computer data'[27] but not providing a definition for cybercrimes. This causes great concern as this Convention is for the purpose of cybercrime yet no definition has been provided in order to maintain clarity and understanding.

The attempts discussed above provide various definitions of cybercrime but the results remain the same in that there is still not a sufficient definition and this is because these definitions accommodate the technological aspect of the offense but do not describe the elements of the crime and what it essentially constitutes.

1.4 Current South African Legislation

To address such crimes, South Africa has instituted some legislative measures which include the Prevention of Organised Crime Act[28] the Financial Intelligence Centre Act,[29] the above mentioned ECT Act and RICA.

This dissertation focuses on these measures and analyses them to establish what the problems are with the existing legislation and whether or not such problems have been addressed in the Bill on Cybercrime. More specifically the dissertation examines the limitations and successes of these measures in combatting cybercrimes and areas where such limitations could be better addressed.

With the legislation which has been introduced in South Africa to address cybercrimes and in particular pertaining to the ECT Act has been criticised enormously.[30] Before the commencement of the ECT Act, the common law and statutory law applied to online forms of

24 Maat (2004)210.

25 Budapest, 23, XI.2001. Herein after referred to as the 'Budapest Convention'.

26 'Computer system' as defined in Article 1 of the Budapest Convention, means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.'

27 'Computer data' as defined in Article 1 of the Budapest Convention, means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.'

28 Act 38 of 1999, herein after referred to as 'POCA'.

29 Act 38 of 2001, herein after referred to as 'FICA'.

30 See M. Kufa 'Cybersurfing without boundaries: The relationship between evidence and computer crime.' De Rebus, December 2008.

offences such as indecency, fraud and *crimen injuria*.[31] However the common law was ineffective in addressing crimes such as theft, extortion, spamming and phishing.[32] When looking at the main aim of the ECT Act, it specifically aims to provide for the facilitation and regulation of electronic communications and transactions.[33] In addition, the ECT Act provides for crimes which are punishable offences within the Act.[34] However, criminal sanctions in the ECT Act have been criticised for not being severe enough.[35]

It has been suggested by Cassim that harsher penalties need to be prescribed in order to deter cyber criminals.[36] Such criticism is inevitable because new legislation is bound to have shortcoming or loopholes such as not being able to deal with constant development of technology as the crimes evolves and become more prevalent. Currently in South Africa, in attempt to address these loopholes a Proposed Cybercrimes and Cybersecurity and Related Matters Bill with a Consultation Document 2015 has been published for comment.[37] In this dissertation a discussion is provided on how this Bill addresses the identified shortcomings and the extent to which it will overcome the shortcomings of the other legislation.

1.5 Conclusion

Cybercrime has been defined by different scholars but there is yet to be consensus on a universally accepted definition. The crime has been interpreted in many different aspects, which vary from the computer itself mainly being the target of the offence or simply as an enabling tool to commit the various offences that are found in traditional criminal law and computer related economic crimes.

One cannot deny that the technological revolution which started with the introduction of computers in the 1950's to the development of the internet in the 1980's, this in itself has given rise to a host of new developments such as social media and cloud computing, brought about the dynamics in crime as well as new dangers. Criminals and terrorists have recognised the potential of the internet and have exploited it. This goes as far as the fact that they may never even have to meet each other in person , yet are still able to commit criminal offences by using encrypted electronic communications to evade government surveillance.[38]

31 Cassim (2012) 360.

32 Ibid.

33 Ibid.

34 The ECT Act sections 86-89.

35 D. Van Der Merwe et al *'Information and communications technology law'* (2008) 77-78. For applicable sanctions see section 89 of the ECT Act.

36 Cassim (2009) 59.

37 Discussion of the Cyber Crimes and Cybersecurity Bill 2015, available at www.justice.gov.za (accessed 20 October 2015).

38 Leslie (2014) 27.

There is no doubt that the term 'cybercrime' has no universally accepted definition, but what has been accepted is that the role of computers can be characterised in one of three ways: firstly the computer can be used as a tool in committing criminal activity, secondly the computer being used as a storage device to store large amounts of stolen or illegally obtained information and lastly the computer can be the target of a criminal activity.[39]

This unresolved dispute creates loopholes such as being able to clearly identify if and when the crime has been committed. This dissertation will address the developing position of cybercrime legislation. It analyses the development of South African legislation from the common law position to the analysis of the Proposed Cybercrimes and Cybersecurity Bill and specifically how the Proposed Bill addresses the criticisms identified from the current legislation in force. In chapter 2 the discussion focuses on the development of the legislation in South Africa addressing cybercrime and the effectiveness of such legislation.

39 Ibid.

Chapter 2: Cybercrime Legislation in South African and its Effectiveness

2.1 Introduction

It is no secret that cybercrime is rapidly evolving and thriving world-wide. Cyber criminals are using sophisticated techniques to steal data and people's identities, to defraud mobile phone users and perform and execute corporate espionage, among other criminal activities.[40]

According to the Federal Bureau of Investigation (FBI), South Africa has been listed as the sixth most targeted country with spear-phishing.[41] Hackers have targeted South African government entities, financial enterprises, banks and other private industry entities with malware and other cyber threats.[42] Further to this, South Africa has the third-highest prevalence of cybercrime in the world after Russia and China, with between 80% and 84% of residents having fallen victim to some form of cybercrime.[43] Almost three quarters of users in South Africa fall victim to scams, online fraud and other forms of cybercrime in the twelve months covered by the report.[44] Symantec estimates that cybercrime affects 2.39 million South Africans a year, with an annual cost of $3.7 billion.[45]

Based on the brief indication of the above findings it is evident that there is a need for improved and more robust laws to deal with cybercrime. With that being said the question one should ask is what was or what is South Africa's position regarding the regulation of these new and evolutionary forms of crime. This chapter aims to answer this question.

2.2 Position of Common Law

Cybercrime differs from crimes committed in a physical medium. The electronic medium challenges the laws designed for a physical medium.[46] In many instances the laws pertaining to 'physical' crimes cannot be extended to address offences committed by means of electronic medium.[47] The reason for this is that a cybercrime offence does not need to have a physical

40 G. Gordon 'The hidden economy of cyber-crime' *Sunday times* 12 February 2012.

41 'Spearphising' is like phishing but tailored for a specific individual or organisation.

42 M Sulfab ' Challenges of cybercrime in South Africa', research paper for Master of Arts in national security studies, American Military University (2014) 9.

43 *Ibid.*

44 *Ibid.*

45 *Ibid.*

46 M Watney 'The evolution of legal regulation of the internet to address terrorism and other crimes' (2007) 3 *Tydskrif vir die Suid-Afrikaanse* Reg 469.

47 *Ibid.*

element to be committed or accomplished. Online crimes are not limited and cannot be contained within the national borders of a country.[48]

The South African criminal law is in the fortunate position of still having and developing the common law system, which because of its emphasis on flexible and adaptable general principles rather than on multiplicity of rigid rules, can reasonably be expected to adapt more easily to new legal phenomena.[49] However, whether South African common law regarding crime in general has successfully adapted to the coming of the computer is a more controversial subject.[50] Even though certain forms of theft are now dealt with by means of statute, the basic common law crime of theft remains and has to be applied even to cases of computer based theft. The same applies to other common law crimes of dishonesty, for example, in cases involving computer based fraud.[51]

One thing that has changed is the fact that the definitional scope of such crimes can no longer be expanded easily.[52] This is because of the so called 'legality' principle, *nullum crimen sine lege,* which has been made part of the inalienable human right bestowed by South Africa's Constitution.[53]

In South Africa, prior to the enactment of the ECT Act, the common law and statutory law at that time was extended as widely as possible so as to cater for the arrest and successful prosecution of some online offenders. However, the applicability of the common law has its own limitations and narrows significantly when dealing with online crimes.[54] For example, when looking at the crimes of breaking and entering with the intent to steal as well as the crime of malicious damage to property, two commonly known categories of computer crimes come

48 *Ibid.*

49 D Van Der Merwe; A Roos; T Pistorius; S Elselen; S Nel *'Information communications and technology law'* (2016) 69.

50 *Ibid.*

51 Van Der Merwe (2016) 69.

52 *Ibid*.

53 Section 35 of Act 108 of 1996.

54 S Snail 'Cybercrime in South Africa- Hacking, Cracking and Other Unlawful Online Acts' (2009) 1 *Journal of information, law and technology* 3.

to mind. On the one hand hacking[55] and cracking[56] and on the other hand the production and distribution of malicious codes known as viruses,[57] worms[58] and Trojan horses.[59]

In the case of S v *Howard*,[60] the court held that the crime of malicious damage to property could apply to causing an entire information system to break down. Even in this instance where the court successfully extends the definition of damage to property of IT systems; there are limitations, which still exist. A major limitation is the element of property which is defined to include corporeal moveable's or immoveable,[61] this being a limitation in that crimes such as hacking and cracking does not necessarily entail corporeal property which has been damaged.[62] To address the limitations of the common and statutory law, the South African Law Commission (SALC) had work in two incremental stages. The first stage investigates whether unauthorised access to computers and unauthorised modification of computer data and software applications could adequately be dealt with by the South African common law, and if not, the second stage would be applied and this would entail whether legislation in this regard was required. The SALC found that the extension of existing common law crimes by the courts was unlikely and that legislation was required.[63]

The question of the adaptability of South African common law has been explored by a number of South African authors. It has been argued that there was a gap in the law as far as computer crimes and related fields are concerned.[64] Further, questions arose with regard to whether legislation would be necessary to effectively deal with the issue. It was apparent that prior to 2002 the law was alarmingly insufficient and inadequate to deal with the evolution in information technology.[65]

55 F Cassim 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' (2015) *Potchefstroom Electronic Law Journal* 93 defines hacking as the infiltration of a computer resource involving the alteration, deletion or destruction of the information residing therein, facilitating the crime of identity theft.

56 Cracking is defined as an action of trying to get into computer systems in order to steal, corrupt or illegitimately view data www.cybercrime.org.za (accessed 10 October 2016).

57 G Ebersoehn & J Henning in ''(2000) 111 define a virus as a piece of programming code usually disguised as something else that causes some unexpected and, for the victim usually undesirable event which is often designed so that it is automatically spread to other computer users.

58 Ebersoehn & Henning (2000) 112 defines a worm as a type of virus that situates itself in a computer system in place where it can do harm.

59 Ebersoehn & Henning defines a Trojan as a destructive computer programme disguised as a game, a utility or application. A Trojan horse does something devious to the computer system while appearing to do something useful.

60 S v Howard (unreported case no 41/258/02, Johannesburg Regional Magistrates Court).

61 C Snyman 'Criminal Law' (2008) 546.

62 Snail (2009) 3.

63 Van Der Merwe et al (2008) 74-76.

64 Sulfab (2014) 9.

65 *Ibid.*

Van der Merwe[66] is one of the South African authors who suggests two possible solutions for the theft of intangibles where computers are involved. The first solution suggested was for the common law aspect in relation to the law of things to be expanded to include incorporeal among things that may be possessed and owned, and therefore also stolen.[67] The second solution suggested was for the criminal law to extend the category of things that may be stolen to include specifically personal rights and immaterial property rights.

An objection to either of these suggestions could be that such a development would fly in the face of the definitions of 'ownership', 'property' and 'thing' which have been developed through the ages.[68] Another objection lies in the fact that these three concepts stated above, might develop varying content in criminal and private law respectively, if the suggested developments are not harmonised in both fields.[69] The legality principle[70] might provide sufficient grounds for specific objection against the expansion of the subject matter of theft in criminal law.[71]

Due to courts being perceived by the internet community as having a lack of expertise about computer technology, information technology specialists were of the opinion that the courts would not be the best platform to develop policy on cyber law or resolve online disputes.[72] With that being said there was still a great need for the creation of new legislation in that the country had to look at other provisions in developing the criminalisation of offences, which the common law was unable to cater for. The RICA and the ECT Act generally prohibit the unlawful interception or monitoring of any data message that could be used in the prosecution of hackers and crackers.[73]

2.3 Regulation of Interception of Communications and Provision of Communications

Our physical world has become infused with e-communication technologies. Electronic communication paraphernalia have altered modern communication patterns and social

66 D Van Der Merwe 'Diefstel van onliggamlike sake met specifieke verwysing na rekenaars' 1985 *South African Journal of Criminal Law and Criminology* 129.

67 *Ibid.*

68 *Ibid.*

69 *Ibid.*

70 *Nullum crimen sine lege*- 'no crime without a law'.

71 Van der Merwe (2016) 68.

72 Cassim (2009) 45.

73 Snail (2009) 1.

behaviours.[74] The privacy of communications is expressly protected under the Constitution.[75] However, any fundamental right can be limited by means of a law of general application, provided that the limitation is reasonable and justifiable in an open and democratic society.[76] RICA is an Act of general application, which allows for the provisions of Section 36 of the Constitution to apply. Any Act permitting surveillance and monitoring of communications will of course raise privacy concerns. It is however argued that a law of this nature is necessary in any modern country including South Africa, given the threat of terrorism and the criminal usage of certain telecommunications equipment.[77]

The aim of RICA is to help make South Africa a safer country. The objective of RICA is to help law enforcement agencies identify users of mobile phone numbers and track criminals using mobile phones for legal activities.[78] It is clear from the objectives contained in RICA that although its primary focus is assisting law enforcement officers in acquiring information required to combat crime, it also regulates interception and monitoring in the private sphere.[79]

Prior to the enactment of RICA, the Interception and Monitoring Prohibition Act[80] was the most important statutory provision with regard to monitoring. The IMPA prohibited the interception of confidential information, but the act was not applicable in the private sphere.[81] The reach of RICA is wider than that of the previous IMPA, as the act is also applicable to the private sphere. It prohibits the intentional interception or authorisation of an interception of any communication in the course of its occurrence or transmission.[82] There are however, certain exceptions.

Section 2 of RICA constitutes an essential provision in this regard. It states that no persona may: intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept at any place in the Republic, any communication in the course of its occurrence or transmission.

The term communication is defined to include both 'direct' and 'indirect' communication. The term 'direct' communication' is of lesser importance for this study as it refers to actual speech

74 Pistorius T 'Monitoring, Interception and Big Boss in the workplace: Is the devil in the details.' (2009) *Potchefstroom Electronic Law Journal* 2.

75 The Constitution of the Republic of South Africa 1996. Herein after 'the Constitution'.

76 Section 36 of the Constitution.

77 Van Der Merwe et al (2016) 487.

78 Cassim (2012) 389.

79 N, Bawa 'The regulation of the Interception of Communications and provision of Communication relation information Act' www.thornton.co.za (accessed 15 July 2016), 308.

80 Act 127 of 1992. Herein after referred to as the IMPA.

81 T Pistorius 'Monitoring, Interception and Big Boss in the workplace: Is the devil in the details.' (2009) *Potchefstroom Electronic Law Journal* 2.

82 T Pistorius (2009) 6.

or contravention between two persons who are in each other's presence.[83] The definition of 'indirect communication' found in section 1 is of greater importance. It reads as follows: the transfer of information, including a message or any part of a message, whether- (a) in the form of speech, music or other sounds; data, text, visual images, whether animated or not; signals, or radio frequency spectrum; or in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system.

'Indirect communication' includes telephone calls, intranet, internet, facsimile facilities, and private and personal e-mail messages, tracking devices in company cars; SMS messages and voicemail messages. The downloading of information from an internet site or the sending or receiving of an e-mail message, or the message itself, would usually fall within the definition of an 'indirect communication' as this would typically, take the form of the transfer of information in the form of data, text, visual images, and it would typically be transmitted by means of telecommunication systems.[84]

It is also important to note that the prohibition in section 2 refers to the interception of a communication 'in the course of its occurrence or transmission'. This must be read with section 1(2) (a) which states that the interception of a communication takes place in the Republic if, and only if, the interception is effected by conduct within the Republic and the communication is either intercepted, in the case of a direct communication, in the course of its occurrence; or in the case of an indirect communication, in the course of its transmission by means of a postal communication or telecommunication system.[85]

When comparing the penalty provision provided in RICA[86] compared to that of the ECT Act, Section 86 in particular, one can observe the similarity between the two acts. It is in this aspect that the relationship between RICA and the ECT Act are seen and why the legislature had to develop law further than RICA. RICA attempted to address the issues, which were at hand regarding laws that needed to be implemented to criminalise cyber conduct.

The act was limited in its application for various reasons and the most obvious being the cybercrime is constantly evolving in that there are new developments of different kinds of crimes and that has to be addressed. Online crimes are not limited to and cannot be contained within the national borders of a county. Various countries therefore moved from self-regulation

83 *Ibid.*

84 T Pistorius (2009) 7

85 T Pistorius (2009) 9.

86 Section 51.

to legal regulation of conduct on the internet by criminalising certain forms of conduct globally.[87]

2.4 Conventions on Cyber Crime

Before looking at the position regarding the ECT Act and the criticisms thereon, it is important to briefly discuss the reasons for the creation or the establishment of such legislation. When looking at cybercrimes it goes without saying that such crimes have no borders and can be committed anywhere in the world and the perpetrator need not be in the country when committing the offence.[88] This is an issue because with regards to borderless crimes, the aspect regarding jurisdiction becomes a problem in that laws are sometimes conflicting especially considering situations where the cybercrime is committed in another country.[89]

In addition to this, developing countries may not necessarily have the specialised capacities to address the borderless nature of cybercrimes.[90] This emphasises the need for international co-operation to address the global nature of cybercrimes. In order to understand the principle behind the enactment of the ECT Act, a brief discussion will be provided firstly on the Budapest Convention[91] and secondly on the African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa.[92]

An important question, which needs to be asked when dealing with cyber laws is not necessarily what the faults are of the state cybercrime laws, but whether the states are effective in an electronic and global medium such as the internet and in general cyberspace.[93] Watney writes that state cybercrime laws should encompass more than just merely criminalising unlawful conduct, but also deal with procedures in the prevention, detection and investigation of crime and collection of evidence for prosecution.[94] She adds that cross border crime affects many jurisdictions and in respect of law enforcement co-operation, issues such as sovereignty and dual criminality may become stumbling blocks, therefore there is an urgent need for harmonisation of laws in respect of cybercrime prevention, detection, investigation and prosecution.[95] The only treaty at present that may be used as a guideline for such

87 Watney (2007) 469.

88 Cassim (2009) 38.

89 *Ibid.*

90 *Ibid.*

91 The Council of Europe on Cybercrime, Budapest Convention , 23 XI.2001.

92 African Union Convention on the Establishment of a Credible Legal Framework for Cyber security in Africa. Herein referred to as AUCLCS.

93 Watney 'Cybercrime Regulation at a Cross-Road: State and Transnational laws versus Global laws' *International conference on Information society* (2012)71.

94 *Ibid.*

95 *Ibid.*

harmonisation of laws is the Council of Europe's Convention on Cybercrime (2001) (the COE Convention).[96]

2.4.1 Council of Europe's Convention on Cyber Crime

The COE Convention was the first instrument at an international level to provide a sound basis for the essential cross border law enforcement co-operation to combat cybercrime.[97] Chapter 2 of the COE Convention aims at criminalising offences that compromise the confidentiality, integrity and availability of computer data and systems.

In particular Chapter 2 articulates that each party must establish as a criminal offence under its domestic laws, when committed intentionally, measures to be taken at national level regarding substantive criminal law. This consists of (1) offences against the confidentiality, integrity and availability of computer data and systems[98]; (2) computer-related offences;[99] (3) content related offences;[100] (4) offences related to infringement of copy right and relate right[101] and (5) ancillary liability and sanctions.[102]

There are basic principles which the COE Convention, to which South Africa has signed but not yet ratified, obliges member states to incorporate cybercrime into their domestic laws.[103] The COE Convention is the first international convention on crimes via the internet and other computer networks.[104] In addition, the resulting cybercrimes convention has three aims: (1) to lay down common definitions of certain criminal offences, thus enabling relevant legislation to be harmonised at national level; (2) to define common types of investigative powers better suited to the information technology environment thus enabling criminal procedures to be brought into line between countries and (3) to determine both traditional and new types of international co-operation thus enabling co-operating countries to rapidly implement the arrangements for investigation and prosecution advocated by the convention.[105]

96 Watney (2012) 72.

97 R. Broadhurst '*Developments in the Global Law Enforcement of Cyber-crime, Policing*: *An International Journal of Police Strategies & Management*' (2006) 409.

98 Budapest convention Chapter 2, Title 1. This consists of illegal access (Article 2), illegal interception (article 3), data interference (article 4), System interference (article 5) and Misuse of devices (article 6).

99 Title 2. This consists of computer-related forgery (article 7) and computer related fraud (article 8).

100 Title 3. This includes offences related to child pornography (article 9).

101 Title 4, article 10.

102 Title 5. This includes; the attempt and aiding or abetting (article 11), corporate liability (article 12) and Sanctions and measures (article 13).

103 S. Snail 'Cybercrime in South Africa and international perspectives' – Presentation held at LSSA AGM 2015.

104 Cassim (2009) 42.

105 Broadhurst (2006) 419 and the Preamble of COEC.

Notwithstanding the fact that the COE Convention can be regarded as international best practice, it should be noted that there are regional/continental initiatives that have been taken.

2.4.2 AU Convention on the Establishment of a Credible Legal Framework

The African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security (2013) (AUCLCS) addresses, in particular, the need for cyber legislation on the African continent. According to Snail,[106] the AUCLCS seeks to harmonise African cyber legislations on e-commerce, personal data protection, cybersecurity promotion and cybercrime control, however, the focus is more on cybersecurity and cybercrimes.

Article III of the AUCLCS makes provision for cybercrime. In particular, it makes laws prohibiting cybercrime, it promotes harmonisation, it makes provision for the double criminality principle, and encourages international co-operation.[107] In addition, the AUCLCS differentiates and proposes amendments to existing laws such as offences specific to information and communication technologies, offences relation to electronic message security measures, proposes adapting certain information and communication technologies offences and proposes adapting certain sanctions to the information and communication technologies.[108]

When looking at all the above mentioned aspects, purposes and objectives of the discussed conventions, one can clearly and easily identify the same objectives and purpose for the basis of the ECT Act. An example of this would be that under the COE Convention, member states are obliged to: criminalise the illegal access to computer systems, illegal interception of data to a computer system and interfering with computer systems without right and intentional interference with computer data without right.[109] What is more, the objectives can purposes of the ECT Act introduces the criminalisation of the above aspects mentioned under the COE Convention.[110]

2.5 Electronic Communications and Transactions Act

Prior to the promulgation of the ECT Act, a problem stemmed from the *nullum crimen sine lege* principle, which provides that no action shall be punishable as a crime unless it

106 S. Snail, 'The African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa' (2011) *Without Prejudice* 1.

107 *Ibid.*

108 *Ibid.*

109 Budapest, 23 XI.2001, 65-69.

110 See chapter 13 of the ECT Act.

constitutes an offence in terms of existing laws.[111] In terms of the Constitution of South Africa, every accused person has the right to a fair trial, which includes the right not to be convicted for an act, or omission that was not an offence under national or international law at the time when the offence was committed.[112]

The extension of the scope of application of certain existing common law and statutory crimes by means of analogy to include cyber offences would have been extremely difficult due to this right that is entrenched in the Constitution.[113] Certain South African authors and legal scholars therefore called for legislation to criminalise cybercrime and law relating to the subject changed dramatically with the enactment of the ECT Act.[114] The ECT Act addresses the facilitation and regulation of electronic communications and transactions in the public interest.[115] It is the primary piece of legislation, which governs the substantive regulation of the electronic communications industry in South Africa. Chapter 13 specifically deals with the regulation of cybercrime; it introduces statutory criminal offences relating to information systems and includes unauthorised access to data and interception or interference with data.[116]

The ECT Act also criminalises other undesirable actions on the internet.[117] Section 85 provides that the definition of 'access' includes the actions of a person who, after taking note of any data becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data. The ECT Act further provides for offences, which are punishable within the context of the Act. The provisions are clearly articulated in the following sections:

> Section 86 addresses unauthorised access to interception of or interference with data. Under the provision section 86(1) it stipulates that a person, who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.
>
> Section 86(2) provides that a person who intentionally and without any authority to do so, interferes with data in a way, which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.
>
> Section 86(3) states that a person who unlawfully sells, offers to sell, procures for use, designs, adapts for use, distributes or possess any device, including a computer programme or a component, which is designed primarily to overcome security

111 Snyman (2008) 39.

112 The Constitution section 35(3) (1).

113 Snyman (2008) 41.

114 Maat (2004) 6.

115 ECT Act section 2(1).

116 ECT Act sections 86(1) – (5).

117 ECT Act section 87.

measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

Section 86(4) defines the fourth offence as when a person utilises any device or computer program mentioned above in order to unlawfully overcome security measures designed to protect such data or access thereto.

The last offence provided for is found in section 86(5), which provides that a person commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

Section 87 of the ECT Act addresses computer-related extortion, fraud and forgery. Firstly it provides that a person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any lawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence. Secondly the section provides that any person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence.

Section 88 of the ECT Act addresses attempt, and aiding and abetting. The first part of this section provides that a person who attempts to commit any offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in sections 89(1) or (2), as the case may be. The second part of the section provides that any person who aids and abets someone to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties as set out in sections 89(1) or (2), as the case may be.

Lastly section 89 of the ECT Act provides penalties for the above mentioned offences committed. Firstly it states that a person convicted of an offence referred to in sections 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months. Secondly that a person convicted of an offence referred to in sections 86 (4) or (5) or section 7 is liable to a fine or imprisonment not exceeding five years.

Therefore the ECT Act, Chapter 13 in particular, criminalises the following conduct as cybercrimes. Firstly, section 86(1) read with the penalty clause in section 89(1) contains an anti-hacking and anti-interception provision that criminalises unauthorised access to a

computer or computer system, or the interception of information.[118] When information is sent over the internet, the information is broken up into packages and these packages of information may be intercepted and copied before they reach their destination. This unlawful conduct may be carried out by means of 'packet sniffing'[119] which may be used to obtain bank particulars.[120] In terms of section 89(1) a fine or imprisonment for a period not exceeding 12 months may be imposed on conviction.

Secondly, conduct aimed at modification of information is also criminalised.[121] Section 86(2) read with the penalty clause in section 89(1) contain an anti-modification provision that makes unauthorised and intentional interference with information that results in the modification, destruction or ineffectiveness of the information a crime, such as the use of viruses, worms or Trojan horses or the defacement of a website. The destruction of the information does not have to be permanent. [122]

The third conduct circumvents security. Sections 86(3) and 86(4) introduce new forms of crimes called anti-cracking and hacking, which prohibits the selling, designing or producing of anti- security circumventer technology. Section 86(3) read with penalty provision in section 89(1) and section 86(4) read with the provision in section 89(2) contain anti-cracking provisions. Section 86(3) makes it a crime to sell, distribute or possess any device, which includes a computer program, that is designated to overcome security measures for the protection of information. Section 86(4) makes it a crime if the anti-cracking device is used. The penalty for the use of the security device is either the imposition of a fine or imprisonment not exceeding 5 years according to section 89(2).[123]

Fourthly, conduct which amounts to a denial or a distributed denial of service attack, is prohibited in terms of section 86(5) read with the penalty provision in section 89(2). Section 86(5) makes it a crime to interfere with an information system so as to constitute a denial of service, even if it is a partial denial of services for legitimate users.[124] Denials of Service attacks are defined as attacks that cause a computer system to be inaccessible to legitimate users.

118 Cassim (2009) 59.

119 'Packet sniffing' is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network.

120 Cassim (2009) 59.

121 ECT Act section 86.

122 Cassim (2009) 59.

123 S. Papadopoulos; S. Snail, *'Cyber@Law SA'* (2012) (3rd ed) 343-346.

124 ECT Act section 86(5) read with section 89(2).

These actions include unauthorised access, unauthorised modification or the utilisation of a programme or device to overcome security measures.[125]

The Fifth conduct amounts to computer-related extortion, fraud and forgery. Section 87(1) read with the penalty provision in section 89(2) provides that a person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any unlawful propriety advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence.[126] An example of the implementation of the penalties which are imposed in the ECT Act is the case of *S v Douvenga*[127] the court had to decide whether an accused employee, GM Douvenga of Rentmeester Assurance Limited was guilty of a contravention of section 86(1) of the ECT Act. It was alleged in this case that the accused intentionally and without permission to do so, gained access to data which she knew was contained in confidential databases and or contravened the provision by sending this data per e-mail to her fiancé' to keep. The accused was found guilty of contravening section 86(1) of the ECT Act and sentenced to R1000-00 fine or imprisonment period of three months. These penalties have been criticised as not being stringent enough to deter cyber criminals.[128]

When analysing the ECT Act, one has to mention the aspect of jurisdiction as cyber-crime is often committed across borders and such a factor needs to be addressed. Section 90 of the ECT Act provides in this regard that a court will have jurisdiction where: an offence was committed in the Republic, any act or preparation towards the offences or any part of the offence was committed in the Republic or, where any result of the offence has had an effect in the Republic, the offence was committed by a citizen of the Republic or a person with permanent residence in the Republic or a person carrying on business in the Republic, and the offence was committed on board any ship or aircraft registered in the Republic or on voyage or flight to or from the Republic at the time that the offence was committed.
It seems as if the ECT act has given minimum compliance with the COE Convention but is also lacking in terms of the resultant protocols of the COE Convention that other jurisdictions have progressed regarding this aspect.

125 Cassim (2009).

126 ECT Act section 87(1) read with section 89(2).

127 District Court of the Northern Transvaal, Pretoria, Case no 111/150/2003, 19 August 2003, unreported,

128 Cassim (2012) 397.

2.6 Measures taken by the United States of America (USA)

Internationally countries have enacted legislation to deal with cybercrimes and problems associated therewith. For a comparative perspective the following discussion briefly examines the measures taken by the USA in order to address cybercrimes and cyber terrorist threats. The USA was probably the first county to enact legislation at a federal state level. The USA has not only been at the forefront of the development of computer technology, but also suffered most at the hands of computer crime.[129] In reaction, the state legislatures have rushed to the scene with legislative guns blazing, although the federal legislatures have been more cautious.[130]

Tapper[131] pointed out the ways in which dealing with the development of such crimes had occurred.[132] He explained that it occurred in two stages.

> The first stage consisted of criminalising the theft of trade secrets and the second step was computer legislation which the state legislatures chose to move on to as this was more inclusive.[133] An example of the stage legislation enacted in attempt to address the development of cybercrime is the Colorado Computer Crime Act.[134] This Act provided a wide definition of 'property' capable of being stolen.[135] For this reason, the Act was criticised on several grounds, particularly that it was too widely framed which went against the legality principle of *nullum cimen sine lege* and also that it seemed to mix both paper and electronic forms of data with that of criminal law.[136]

During the mid-1980's the US Congress passed two criminal statues to combat computer related crimes in which federal interests are involved.[137] These were the Counterfeit Access Device and Computer Fraud and Abuse Act[138] (CFA Act) and the Electronic Communications Privacy Act[139] (ECP Act). The ECP Act was enacted to include the digital transmission of

129 Van der Merwe et al (2016) 93.

130 *Ibid.*

131 C. Tapper 'Computer law' (1990) (4ed) 301.

132 *Ibid.*

133 *Ibid.*

134 Colorado Computer Crime Act of 1973

135 'Property capable of being stolen: financial instruments, information, including electronically produced data and computer software and programs in either machine or human readable form, and any other tangible of intangible item of value.'

136 Van der Merwe et al (2016) 93.

137 Van Der Merwe et al (2016) 94.

138 Counterfeit access device and computer fraud and abuse act of 1984(18 usc 1030).

139 Electronic communications privacy act of 1986 (18 usc 2510-2711).

electronic data to broaden the government's power to tap into private communications.[140] The case of the *US v Councilman*[141] thoroughly tested its provisions. In this case, the defendant was the vice president of a company called Interloc Inc.; its business consisted of online listing of rare and out of print books.

The legal problem emerged from the councilman directing Interloc employees to intercept email traffic directed to Amazon.com. The prosecution alleged that the purpose of these interceptions was to develop a list of the most wanted books, gain strategic commercial information about possible competitors and thus to gain strategic advantage.[142] The councilman responded by saying that his firms actions did not contravene the prohibition on the interception of electronic communications because the email messages were in an electronic storage.[143]

The District Court held that the councilman was correct and was supported by the Appeal Court. However, the court hearing the special application reversed the decision and held that it was not the legislature's intention to exclude electronic storage from the definition of electronic communications. Thus the court held that the councilman's employees did contravene the prohibition on the electronic communications. When comparing the ECP Act, to the South Africa Legislation namely the ECT Act, this problem would have been solved in that 'a stored record' is contained in the ECT Acts definition of 'data'.[144] On the other hand, American courts make a much more watertight division between data store and data travelling.[145]

A popular prosecution within the application of the ECP Act is the case of *US V Kevin Mitnick*.[146] Mitnick began his criminal career as early as 1981 by stealing computer manuals at the age of 17. In 1988 at the age 25, Mitnick monitored MCI and digital equipment security officials. When he was discovered, he was charged with causing damage amounting to four million dollars to computer operations and stealing software worth one million. Mitnick was convicted and revived 1 year jail sentence. In 1994, he broke into Tsotumu Shimomura's computer system at the San Diego Super Computer Centre. In 1995 Shimomura and federal agents traced the signal of a cellphone that Mitnick was using at that time this led to his two

140 Van der Merwe et al (2016) 94.

141 US v Councilman Court of Appeals no 131083 (2005).

142 Van der Merwe et al (2016) 95.

143 *Ibid.*

144 'Data' means electronic representations of information in any form, as defined in section 1 of the ECT Act.

145 Van der Merwe et al (2016) 96.

146 G. Barker 'Trespasses will be prosecuted: computer crime in the 1990's' (1993) 1 *Computer Law Journal* 72 ff.

year sentence during 1997, of which he was convicted of repeated parole violations and using cellphone numbers to dial into computer databases. Mitnick was finally sentenced for a longer period of 46 months in a federal prison after pleading guilty to computer fraud and wire fraud, specifically for breaking into computers, intercepting communications and stealing proprietary software from cellular telephone companies.

The CFA Act had two incarnations namely 1984 and the amended form of 1986. The 1986 Act added three new offences: (a) theft of property by use of a computer as part of a scheme to defraud; (b) malicious damage felony which penalises illegal access to a federal interest computer and altering or damaging or destroying information on it; (c) preventing the authorised use of a computer.[147] The crimes specified in paragraph (c) includes crimes similar to those created by section 86(5) of the ECT Act, in particular denial of service attacks.[148] There have also been prosecutions within the application of the CFA Act. In the *US v Czubinsla*[149] case, the accused was an employee of the US Internal Revenue Service. The accused accessed the private files of some of his colleagues out of mere curiosity. The accused was found guilty in the court of first instance. The Circuit Court of appeal reversed his conviction by the court of first instance on the basis that the prosecution had failed to show that he had obtained anything of value.[150]

In 1996, the National Information Infrastructure Protection Act was promulgated which protects individuals against various crimes involving protected computers. Federal offences include cyber fraud, identity theft, spamming, cyber stalking, making intentional false representations online, the use of password sniffers, the decimation and creation of worms as well as the writing of viruses and Trojan horses, website defacements and web-spoofing.[151]

The terrorist attacks of 9 September 2001 changed the legislative landscape.[152] The Patriot Act[153] was enacted to respond to the 9/11 attacks on the World Trade Centre and Pentagon.[154] The main stated purpose of this Act is: 'to deter and punish terrorist acts in the US and around the world, to enhance law enforcement investigatory tools and for other purposes.'[155] This Act

147 Van der Merwe (2016) 95.

148 'Denial of service attacks'- these are attacks that cause a computer system to be inaccessible to legitimate users. see also Van Der Merwe et al (2016) 79.

149 *United States v Czubinskli* 106 f 3a 1069 (1st Cir 1997)

150 Van der Merwe (2016) 95.

151 Cassim (2009) 43.

152 Van der Merwe(2016) 96.

153 The USA Patriot act of 2001 (United and strengthening America by providing appropriate tools to intercept and abstract terrorism'.

154 Cassim (2016) 46.

155 Van der Merwe (2016) 96.

incorporated the provisions of two earlier anti-terrorism bills; it considerably extends the states prosecutorial powers and has been used in many post 2001 prosecutions of suspected terrorists.[156] On 9 March 2006, President Bush signed the USA Patriot Improvement and Reauthorisation Act of 2005. In the form of a progress report of five years on the Patriot Act, the President launched the co-operation between law-enforcement and intelligence agencies that the Act had managed to achieve.[157]

The Cybersecurity Act[158] was an effort by Congress to address the cyber threat and cybercrime facing the public and private sectors in the US.[159] This Act was jointly introduced by former Senator Lieberman and Senator Collins in the Senate Homeland Security and Government Affairs Committee, was the latest and most comprehensive attempt to enhance the nations cyber security capabilities.[160]

In the USA, there is currently one of the biggest cybercrime cases which have been filed in history known as the *New Jersey Case*. In this case, five men have been arrested and have been charged with hacking and credit card fraud spree that cost most companies more than 3 hundred million rand.[161] The five men hid their efforts by disabling anti-virus software and storing data on multiple hacking platforms. They sold payment card numbers to resellers, who then sold them online forums or cashers who encode the numbers onto blank plastic cards. There are numerous charges that the five men are being charged with and this case is still pending.

This is an example of how cybercrime is developing and affecting countries such as the USA who have laws in place to address such crimes. Valid attempts have been made and are continuously being improved in the USA to respond to the increase of cybercrimes.

The enactment of the Patriot Act and the other measures demonstrates the US government's commitment to combat international cybercrime. Further the introduction of the Bill also illustrates that the USA is taking the lead in updating out dated computer crime laws to keep abreast with advancing computer technology.

156 Van der Merwe (2016) 97.

157 *Ibid.*

158 Cyber Security Act of 2012.

159 Sulfab (2014) 50.

160 Had this Bill been enacted into law, the first version of the bill in 2012 would have granted new powers to the Department of Homeland Security to oversee us government cyber security.

161 Newark, Boston U.S indicts hackers in biggest cyber fraud case in history, www.reuters.com (accessed 25 May 2016).

For South Africa, the introduction of the ECT Act as the key legislation to ensure a secure information society was a significant step in the right direction. It seeks to provide legal recognition to electronic transactions and prevents unwarranted abuse in cyber space.[162] The ECT Act had defined a number of conducts that constitute cybercrime and establishes several procedures to enhance the enforcement of the Act by law enforcement authorities.[163] The fight against cybercrime will remain an active battle between the law enforcement agencies and cyber criminals.

2.7 Problems or Shortcomings in relation to the ECT Act

Although the ECT Act goes a long way towards addressing cybercrime in South Africa, there is room for improvement particularly with regard to addressing the prosecution and the penalties which has been imposed on the cyber criminals. South Africa needs to prescribe harsher consequences to deter cyber criminals.[164] The feasibility of introducing collaborative initiatives involving the police, the private sector and academia to combat cybercrime should also be explored, as it is important to involve all the role players in the fight against cybercrime.[165]

These penalties have been criticised as not being stringent enough to deter cyber criminals.[166] Therefore, the argument here is that the ECT Act penalty clause is required to be amended to reflect stricter punishment against would be cybercriminals to reach their full potential.[167] Further criticism is that the ECT Act promises a new development in the specialised investigation of cybercrime by creating cyber-inspectors and to date no cyber inspectors have been appointed.[168]

2.8 Conclusion

It is noteworthy that RICA was the first piece of legislation to address aspects of the law for which the common law was inadequate. It recognised laws which needed to be implemented to criminalise cyber misconduct. RICA however, had limitations in its application due to the constant new developments of cybercrimes which needs to be addressed. These limitations have led to new legislation being developed.

162 Sulfab (2014) 54.

163 *Ibid.*

164 Cassim (2009) 68.

165 *Ibid.*

166 *Ibid.*

167 Sulfab (2014) 41.

168 Van Der Merwe et al (2016) 80-81.

It needs to be said that the ECT Act is a move in the right direction to dealing with cybercrime in South Africa. An example of this is the case law which has been mentioned and how the cases have addressed the application of the ECT Act and the outcome thereof. However, there is room for improvement.[169] It has been submitted further that most provisions on cybercrime in the ECT Act are noble endeavours, but their enforceability is still to be tested in South African courts.[170]

Given the borderless nature of the internet and the challenges that it poses in terms of jurisdictional questions, international co-operation and uniformity, it is important that states learn from one another's efforts to deal with cybercrime and create an international cybercrime code to be applied universally if any significant success is to be achieve in combatting cybercrime.[171] South Africa can learn from the approach which the USA has followed particularly their initiative to develop and enhance their laws relating to cybercrimes and cybersecurity and the measures developed to predict computer related threats.

It is clear that the ECT Act is an important legal development that will influence a multitude of legal transactions and documents. Although the ECT Act is not without flaws and many concerns have been raised during its making, it can be regarded as an important step in creating a more secure and legally certain environment for electronic commerce, which can definitely contribute to the economic growth of South Africa.[172]

Chapter 3: Cybercrime and Cybersecurity and Related Matters Bill

169 Cassim (2009) 68.

170 *Ibid.*

171 Cassim (2009) 63.

172 J. Coetzee 'the Electronic Communications and Transactions Act 25 0f 2002: facilitating electronic commerce.' (2004) Stellenbosch Law Report 501.

3.1 Introduction

The purpose of this chapter is to discuss the application and effectiveness of the recently published Cybercrimes and Cybersecurity and Related Matters Bill[173] in relation to the applicable sections which have been discussed in Chapter 2 of this dissertation. Further the chapter explores whether or not the Bill addresses the shortcomings which have been identified in the ECT Act. Further to this, if it does address the shortcomings how; including the opinions of academics on this matter.

Most cybercrime acts are estimated to originate in some form of organised activity, with cybercrime black markets established on a cycle of malware creation, computer infection and botnet management.[174] This includes the harvesting of personal and financial data, data sale and selling of financial information which are reasonable simple to carry out. Cybercrime perpetrators no longer require complex skills or techniques.[175] Globally, cybercrime shows a broad distribution across financially driven acts and those relating to computer, as well as acts against the confidentiality, integrity and accessibility of computer systems. However, globally police recorded crimes statistics do not represent a sound basis for determining the precise impact of cybercrimes.[176]

According to Cassim cybercrime differ from other crime in that it operates within a highly organised system making it more likely to create beneficial effects that outweigh its costs, and the perpetrators usually possess a particular psychology that make them almost immune to more innovative law enforcement method. [177] For example the use of the internet to facilitate and commit acts of terrorism is a real occurrence that often can only be dealt with after the event, with the perpetrators even literally getting away with murder. Cyber-attacks are typically intended to disrupt the proper functioning of the target, such as computer systems, servers or underlying infrastructure, especially if these systems are part of critical information infrastructures of a country, among others, by means of unlawful access, computer virus or malware.[178] With the above having been said, it will be imperative to examine the scope and application of the Bill.

173 Published in Government Gazette, volume 603, 2 September 2015, number 39161, herein after referred to as 'the Bill'.

174 Consultation document on Cyber Crimes and Cybersecurity Bill, www.justice.gov.za (accessed 20 October 2015) 1.

175 Consultation document (2015) 2.

176 *Ibid.*

177 Cassim (2009) 40.

178 Cassim (2012) 385.

3.2 Application of the Bill

The preamble of the Bill on Cybercrime states that its purpose is among other things: *To create offences and impose penalties to further regulate their powers to investigate, search and access or seize; to further regulate aspects of international cooperation in respect of the investigation of cybercrime; to regulate jurisdiction; establishment of various structures to deal with cybersecurity; to regulate National Critical Information; to regulate aspects relating to evidence and to impose obligations on electronic communication service providers regarding aspects which may impact on cybersecurity.*

For purposes of this dissertation only the application of sections 3, 4 and 5 including sections 22 and 23 of the Bill on Cybercrime are discussed. These sections make provision for offences regarding personal and financial information or data related offences, unlawful access and unlawful interception of data that are the provision which have been discussed and have been discussed in Chapter 2 of this dissertation.

Section 3 of the Bill regulates personal and financial information offences of any person who unlawfully and intentionally acquires by any means or possesses or uses or provides this information to another person to another person. The use of personal or financial information of another person for purposes of committing an offence is punishable under the Bill and the offender will be found guilty of such an offence.[179] In addition, any person who is found in possession of personal or financial information of another person to which there is a reasonable suspicion that such information was acquired, is possessed or is to be provided to another person for purposes of committing an offence and is unable to give satisfactory exculpatory account to such possession is guilty of an offence.

The discussion pertaining to this provision is based on the fact that information or data can be the subject of several constitutive acts, namely; the act of obtaining, possessing and using identity related or financial information or data. Personal or financial information or data can be for example, obtained via illegal access to a computer device and database, the use of phishing or interception tools or through illicit acquisition. Examples of this are acts such as dumpster diving,[180] social engineering,[181] theft and online buying of information or data of another person.[182]

179 The Bill on cybercrime, section 3.

180 Dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network.

181 Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. An example of social engineering is phishing and spear phishing.

182 Consultation Document (2015)4.

Further, financial information or data is a popular target in cyberspace. Financial information or data which is targeted in cyberspace is information pertaining to savings accounts, credit cards, debit cards and financial planning information.[183] Personal or financial information or data are mostly used to commit financial cybercrimes. The above mentioned offences provided for in this particular section, aim to address personal or financial information or data related offences.[184]

Section 4 of the Bill regulates unlawful access and criminalises the unlawful accessing of the whole or any part of data, a computer device, a computer network, a database, a critical database, an electronic communications network or national critical information infrastructure.[185] With regards to this section, illegal access is not the end goal to an offence but rather the first step towards further crimes such as interfering with or intercepting data. Since the development of computer networks, its ability to connect has been used by hackers for criminal purposes.[186] Hackers need not be present at the crimes scene; they just need to circumvent the protection securing the database, network or computer device.[187]

The criminalisation of illegal access represents an important deterrent for many other subsequent acts against the confidentiality, integrity and availability of data and related devices.[188] Thus, to address the above mentioned this section criminalises the unlawful accessing of the whole or any part of data or any related device.[189] A legal interest is infringed, not only when a person unlawfully interferes or commits other unlawful acts in respect of data, a computer device, a computer network or database or an electronic communications network, but also when a perpetrator for example, merely accesses a computer network. Illegal access does not require the offender to access system files or other stored data.[190]

Lastly Section 5 of the Bill regulates unlawful interception of data and provides that any person who unlawfully and intentionally intercepts data to, from or in a computer device, a computer network, a database, a critical database, an electronic communications network or a national

183 Consultation Document (2015) 4.

184 *Ibid.*

185 The Bill on cybercrime section 4.

186 Consultation Document (2015) 5-6.

187 *Ibid.*

188 *Ibid.*

189 *Ibid.*

190 *Ibid.*

critical information infrastructure or any part thereof is guilty of an offence.[191] The criminalisation of this act aims to protect the integrity, privacy and confidentiality of data within a computer device, a computer network, a database or an electronic communications network.[192] Unlawful access allows the perpetrator to carry out further actions to acquire data unlawfully. Thus, the use of information communication technologies is accompanied by several risks related to the security of information transfer.

In addition to illegal access, Section 22 of the Bill provides that any person who attempts, conspires with another person; or aids, abets, induces, incites, instigates, instructs, commands or procures another person to commit an offence is in terms of this chapter, guilty of an offence and is liable on conviction to the punishment applicable to someone convicted of actually committing that offence.[193]

Section 23 of the Bill aims to address concerted and organised efforts to commit cybercrimes by providing that if an offence in terms of the Bill is committed in concert with other people it must be considered as an aggravating circumstance for purposes of sentencing.[194]

Various online communities exist in order to facilitate cybercrimes and are sometimes in accordance with their ideological principles.[195] An example of co-operation in cybercrime is where a person obtains information through social media and gives it to a hacker to gain access to a server, on which certain information is copied, it in turn is given it to another person who sells the information or uses the information to commit fraud or computer related extortion. The application of the Bill particularly, provisions which deal with addressing cybercrimes in South Africa, has attempted to address the shortcomings identified in ECT Act.

3.3 How the Bill has addressed ECT Act identified shortcomings

As mentioned earlier this dissertation focuses on sections 3, 4 and 5 of the Bill in comparison to Chapter 13 of the ECT Act and in particular sections 86 to 89.

Firstly Chapter 2 of this paper, briefly looked at the shortcomings of the ECT Act with the following aspects being identified; that the penalties under sections 86 to 89 of the ECT Act are not harsh enough and lastly that there have been promises of cyber inspectors but no

191 The Bill on cybercrime, section 5.

192 *Ibid.*

193 The Bill on Cyber Crime, section 22.

194 The Bill on Cyber Crime, section 23.

195 Consultation Document (2015) 30.

development has occurred in that regard. When looking at the penalties which the ECT Act has imposed, these ranging from a fine or imprisonment not exceeding twelve months, are not considered as harsh penalties and that harsher penalties should be imposed.

The Bill, however, imposes harsh penalties, for an offence that is committed and when the perpetrator is found guilty of the said offence. The penalties range from a fine with a minimum amount of 5 million rand to a maximum of 10 million rand. The period for imprisonment provided for is a minimum of 5 years to a maximum of 10 years. The Bill also makes provision for the imposition of both a fine and imprisonment on conviction.[196] This can be noted as a substantial improvement moving forward from the ECT Act and that the Bill has definitely provided for harsher fines and longer periods of imprisonment.

Secondly when looking at the provisions which the Bill has made with regards to the extent of state control and institutions created, sections 50 to 57 of the Bill provides the structures which deal with cybersecurity. These include Cyber Response Committee, Cybersecurity Centre, Government Security Incident Response Team, National Cybercrime Centre, Cyber Command, Security Hub and Private Sector Security Incident Response Teams.[197] These provisions in the Bill create new state institutions to counter cybercrime and cyber terrorism. These institutions are co-ordinated by a Cybersecurity Committee under control of the State Security Ministry.[198] This is in stark context to see aspect relating to Cyber Inspectors provided for in the ECT Act.

3.4 Commentary on the Bill

Various academics have had different opinions regarding the Bill and the impact the Bill has on the law in South Africa and whether such an establishment will be to the benefit or detriment of the country.

Duncan is of the opinion that the draft law's promise to make the internet a much safer, freer space for South Africans is illusory.[199] Duncan writes that the Bill threatens digital rights in significant ways, especially the freedom of expression and association, and the right to privacy. It is also observed that the Bill lacks important checks and balances, and increases

196 The Bill on Cyber Crime, chapter 2.

197 The Bill on Cyber Crime, sections 50-57.

198 Duncan 'A new Bill threatens our digital rights and raises the spectre of internet censorship.' www.mailandguardian.co.za.

199 Duncan, 1.

state power over the internet in concerning ways in sections 51 to 64 of the Bill provides for significant state involvement in the monitoring of business and private cyber activity.[200]

Duncan adds that the Bill creates a host of new state institutions which fall under several state departments, to counter cybercrimes and cyber terrorism. Hence, Duncan states that the Bill will hand indirect control of the internet to South African spies. Further to this, Duncan says that state security is not the most appropriate institution to be tasked with this responsibility as it leans towards secrecy and its existing activities which lack democratic controls.[201]

He goes further and says that the Bill resists the temptation to over criminalise online behaviours such as spamming and that this remains a ground for concern. In addition, it is noted that the Bill amends RICA by adding additional offences. Duncan states that its drafters argue that the Bill and the Criminal Procedure Act[202] do not contain adequate measures to investigate cybercrimes.[203]

Duncan writes that it does have important public purposes, for instance, that it criminalises acts such as unlawful interception of and interference with data, as well as computer related fraud and cyber terrorism, and regulates foreign co-operation to fight these cries. It protects critical information and infrastructure by making it illegal to interfere with them.[204] He concludes by saying that on a broader level, governments including the South African government need to acknowledge that they have helped to create the enormous problem which they are legislating against. They have vested interest in promoting communications networks that are built for vulnerability rather than for resilience, because they want to maintain their ability to spy on their citizens.[205]

Commentary from the Right2Know Campaign[206] notes that this Bill forms part of a set of laws and policy initiatives in South Africa that aims to regulate the ever expanding online economy, as well as the surge in cyber related crimes (locally and internationally).[207] The Campaign also states that the current legal framework to combat cybercrime is a hybrid of legislation and the common law. The common law however, takes its approach on a case by case basis, thus

200 *Ibid.*

201 *Ibid.*

202 Act 51 of 1977.

203 Duncan, 2.

204 *Ibid.*

205 Duncan, 6.

206 Right2Know campaign: 'Legislation: concerns over proposed cyber law', October 2015 www.Right2knoww.org.za (accessed 20 October 2015).

207 *Ibid.*

has not kept pace with the dynamic nature of cybercrimes. The Right2Know Campaign is of the opinion that the Bill is a product of calls by various stakeholders for government to enact specialised legislation and to align South Africa with international practice.[208]

Furthermore, that if passed the legislation will codify numerous offences or 'cybercrimes and their related penalties. What is more, the Right2Know Campaign says in essence, the Bill criminalises unlawful access to and interception of data; provides local authorities with extensive powers of investigation, search, access and or seizure; imposes various obligations on electronic communications service providers and regulates jurisdiction of the courts, specifically in relation to cross border offences.[209] However, the Right2Know Campaign criticises the Bill in that they state that the seven deadly sins of the Bill are that it:[210]

(1) Hands over control of the internet to the Minister of State Security,

(2) Gives the state security structures the powers to effectively declare 'national key points' of the internet- and potentially grants backdoor access to any network,

(3) Criminalises journalists and whistle-blowers by sneaking in the worst parts of the disputed 'Secrecy Bill',

(4) Increases the state's surveillance powers and is even more invasive than RICA,

(5) Undermines South African's civil liberties and particularly the constitutional rights to privacy,

(6) Contains 59 new criminal offences involving computer usage – many of which are so broad that they could ensnare ordinary computer users, and

(7) Contains anti- copyright provisions so harsh you could be charged for even posting a meme.

The Bill also considers suspects guilty until proven innocent. The Right2Know Campaign suggests that the solution would be to scrap the entire Bill and start from scratch with proper public participation and protection as well as aiming to preserving the democratic spirit of the right to privacy.[211]

Similarly, Tshongweni[212] is of the opinion that currently South Africa has no legislation that addresses cybercrimes, whether it describes what constitutes a cybercrime, how to enforce

208 *Ibid.*

209 Bernstan, Ebrahim, Obane 'Concerns raised over SA cybersecurity law' www.news24.com (accessed 20 October 2015).

210 Right2Know campaign: 'What's wrong with the Cyber Crimes Bill-The seven deadly sins', www.right2know.org.za (accessed 30 November 2015).

211 Ibid.

212 M. Tshongweni, Concerns raised over Cybercrime and Cybersecurity Bill in SA, www.itnewsafrica.com (accessed 22 September 2015).

the law governing cybercrime or to determine appropriate correctional sentencing for those convicted of offences within this realm.[213]

Tshongweni states that the Bill is timeous in that it proposes legislation that will bring South Africa in line with international laws governing internet based crimes. However, Tshongweni is of the view that the Bill is excessively far reaching, beyond practical plausibility in many instances and that it grants a concerning level of discretion to the State's Security Cluster.[214]

The Law Society of South Africa[215] has also made their submissions[216] on the Bill. In this dissertation only a few of their submissions will be noted. LSSA submits that the Bill goes in the right direction in extending the list of substantive cybercrimes which were initially limited in the ECT Act like unauthorised access to, interception of, or interference with data.[217] LSSA submits that the Bill accordingly expands that types of offences originally covered under the ECT Act and also criminalises more activities relating to the unlawful use of computer systems.[218]

LSSA further submits that it is of great concern that the Bill will be amending more than 16 already existing laws, and that there will inevitably be unintended consequences which have to be minimised as far as possible with a longer period of consultation.[219] Furthermore, a Bill of this magnitude should not be rushed through Parliament and it should be able to withstand constitutional scrutiny on aspects of privacy, the right to dignity and freedom of expression. LSSA believes that in the Bill's current state, it will not pass constitutional scrutiny and it ought to be substantially revised.[220] LSSA further states that the Bill does not cover all principles as contained in the COE. LSSA raises concern about the extent to which attention has been provided to harmonise the legislation with that of other countries. Lastly, LSSA submits that greater consultation and research needs to be undertaken by the Justice and Constitutional Department.[221]

213 *Ibid.*

214 *Ibid.*

215 Herein after referred to as 'LSSA'.

216'Comments by the Law Society of South Africa on the Cybercrimes and Cybersecurity Bill', www.lssa.org.za (accessed 30 April 2016).

217 *Ibid.*

218 *Ibid.*

219 *Ibid.*

220 *Ibid.*

221 *Ibid.*

3.5 Conclusion

Firstly that the specific conduct criminalised and any study of cybercrime offences must take into account the Criminal Procedure Act as this is law that deals with issues applicable to all offences.[222]

Secondly, when analysing the functions of cybercrime legislation, there are several aspects which needs to be taken into account, namely; setting clear standards of behaviour for the use of computer devices; deterring perpetrators and protecting citizens; enabling law enforcement investigations while protecting individual privacy; providing fair and effective criminal justice procedures; requiring minimum protection standards in areas such as data handling and retention and enabling co-operation between countries in criminal matters involving cybercrime and electronic evidence.[223] When looking at the above mentioned aspects we have to compare this to the Bill and analyse whether the Bill has met these standards and if so, to what extent.

The last aspect, is comparing whether the Bill has in actual fact addressed the shortcomings identified in the ECT Act. From the preceding discussion, there is a clear indication that the Bill has addressed to a great degree of the shortcomings in that the Bill does provide for harsher penalties than those imposed in the ECT Act.

With regard to the cyber inspectors in the ECT Act which were created but never implemented, the Bill has addressed this issue to the extent that it has created a Cybersecurity Structure under the control of the Director General of State security who will control the regulation regarding cybercrime and cyber terrorism. To this extent the Bill has addressed the shortcomings of the ECT Act. However, with regards to the shortcoming relating to the extent of the state control in relation to the regulation of cybercrimes, the Bill has not addressed these. With reference to the opinions mentioned previously in this chapter, I submit that the state is given extensive control over the regulation of cybercrimes and the contents thereof. In particular the state is provided with too much control over how businesses and private persons communicate over the internet. One can therefore conclude that the Bill has addressed majority of the shortcomings which have been identified in the ECT Act and that, although it has deal with such issues, the Bill has its own shortcomings.

222 *Ibid.*

223 LSSA comments (2016) 52.

Chapter 4: Conclusion and Recommendations

4.1 Conclusion

As we move forward into the information age, it becomes increasingly clear that every nation must have a comprehensive legal framework to combat cybercrime. A criminal armed with a

computer and an internet connection has the capability to victimise people and access private information and computer systems illegally anywhere in the world.[224] A key issue is that cybercrime is not confined within national borders.[225] International cybercrimes have impeded law enforcement efforts in ways never before contemplated.[226]

This dissertation has examined select legislation in South Africa and the provisions within these laws in depth, to determine their impact on existing cybercrime laws. When analysing what the current position is regarding the understanding of what cybercrimes are, the background as explained in the first chapter, provides that there is no uniform definition of cybercrime. Further in the introductory chapter, it is explained that there is an accepted definition provided by Parker but the suggested definition is said to not be sufficient enough as it does not explain what constitutes as a cybercrime.

The second chapter of this dissertation outlined the development of law in South Africa regarding cybercrimes, namely the development from the common law to RICA and the ECT Act. Firstly it was concluded that the applicability of the common law has its own limitations and narrows significantly when dealing with online crimes and that alone calls for development of the law in this regard. Secondly with regards to RICA, the Act attempted to address the issues which were at hand regarding laws that needed to be implemented to criminalise cyber misconduct, but the Act was limited in its application for various reasons and the most obvious being the cybercrime is constantly evolving.

Thirdly the international conventions were compared by way of discussion of their purposes and objectives. It was determined that the same objectives and purpose are the basis of the ECT Act. The forth aspect which was discussed within the second chapter of this dissertation was the position regarding the ECT Act and it was ascertained that the ECT Act is an important legal development that has influence a multitude of the regulation of cybercrimes.
Although the ECT Act is not without any flaws, and many concerns were raised during its development/drafting, it can be regarded as an important step in creating a more secure and legally certain environment for electronic commerce, which can contribute to the economic growth of our country.

224 Leslie (2014) 169.

225 *Ibid.*

226 *Ibid.*

The final discussion which was raised within chapter two of the paper was about the shortcomings identified within the ECT Act. These shortcomings are that penalties which are provided for within the ECT Act are not stringent enough to deter cyber criminals. Further criticism is that the ECT Act promises a new development in the specialised investigation of cybercrime by creating cyber inspectors, and to date not much has come of this because no cyber inspectors have been appointed. To address the identified shortcomings, the Bill was proposed.

Chapter three of this paper discussed the provisions within the Bill which address the shortcomings identified within the ECT Act. With regard to the extensive nature of state control which was provided for in the ECT Act, it was submitted that the state institutions have been created by the Bill are under the control of different state departments to counter cybercrimes and implement cybersecurity this still amounts to extensive state control of private information. The second shortcoming discussed was one relating to the penalties within the ECT Act which were held to not be stringent enough. The Bill successfully addressed this aspect as discussed by imposing penalties which are harsher than those in the ECT Act, if offenders are found guilty of committing offences criminalised within the Bill. The third and final shortcoming identified in terms of the ECT Act, was the provision created cyber inspectors which have never been appointed.

This aspect has been identified by the Bill to the extent that the Bill provides for state institutions which are controlled under different state departments to counter cybercrimes and ensure cybersecurity. It was concluded that the Bill has addressed majority of the shortcomings of the ECT Act but that the Bill has its own shortcomings.

In concluding, an effective fight against cybercrimes requires increased, rapid and efficient international co-operation in criminal matters. The possibility exists that the new forms of cybercrime will emerge with evolving technology and the legislation needs to be created to address such issues both now and in the future. The question is whether the Bill sufficiently caters for this.

4.2 Recommendations

South Africa at present does not have a co-ordinated approach in dealing with cybercrime and does not have a comprehensive cyber defence strategy in place.[227] The complexities of cyberspace and the dynamic nature of technological innovations require a holistic cyber

227 M. Grobler, J. Van Vuuren. J. Zaaiman, 'Preparing South Africa for cybercrime and cyber defines.' (2013) 32.

defence framework. The structures that have been established to deal with cybersecurity issues and the current legal system are inadequate to holistically deal with these issues.[228]
It is suggested that the need for international cyber defence collaboration is crucial.[229] The keys to these collaboration efforts are open communication and a willingness to give and accept input from others.

Watney is of the view that state cybercrime laws should encompass more than merely criminalising unlawful conduct but also need to deal with procedures in the prevention, detection and investigation of crime and collection of evidence for subsequent prosecution.[230]
Watney is of the opinion that the concept 'cybercrime' will have to be re-evaluated because it has been interpreted as an umbrella concept that includes various forms or categories of unlawful conduct.[231]

According to Watney, law enforcement within an electronic medium and specifically a global medium that is accessible to all nation states, face challenges that are dissimilar to that of law enforcement within a physical medium.[232] The medium necessitates the implementation of 'new' laws on a global level which will address the following issues: ensuring all states have cybercrime laws on national and transnational levels in place; harmonising a state's cybercrime laws specifically pertaining to cross border crimes; conceptualise the legal position regarding certain forms of cybercrime and addressing enforcement of these laws.[233]

South Africa can learn from the approaches followed in other countries like the USA, whilst keeping in mind the South African context. Learning should be premise on what is relevant within the South African context and how can it be implemented on a practical level, so as not to become another unimplementable policy.
We can take note of the USA initiative to develop and enhance cyber intelligence and cybersecurity measures to better predict computer related threats and counter act them.[234]

228 *Ibid.*

229 Grobler et al (2013) 34.

230 M. Watney 'Cybercrime regulation at a cross-road: state and transnational laws versus global laws', International conference on information society (2012) 71.

231 Watney (2012) 72.

232 Watney (2012) 73.

233 *Ibid.*

234 Cassim (n 15 above) 404.

According to Sulfab[235] the wide spread and dependence on digital devices had ushered in a new form of cybercrime which requires new legislation. He is of the view that to successfully combat the growing phenomena of cybercrime, the government of South Africa needs to amended and legislate laws to address current issues facing governments and society relating to cyber hacking, cyber terrorism and violation of intellectual property.[236]

Furthermore, he adds that the constant rise and dynamic nature of cybercrime in recent years had required the government of South Africa to establish new mechanisms to address issues related to cyber intrusion and online fraud. While the South African Parliament had successfully enacted the ECT Act, amendments and new laws are needed.[237] The rise in computer related offences over the last two decades had required the South African Government to pay more attention to address issues arising from this.

Cyberspace ultimately belongs to the global world and despite the different and opposing views, all nation states should be in agreement that cybercrime, cyber-attacks and terrorist activities may end the economic and social advantages cyberspace holds for generations to come.[238]

Bibliography

1. Books:

235 Sulfab (2014) 40.

236 Sulfab (2014) 40.

237 Sulfub (2014) 41.

238 M. Watney 'The Way Forward in Addressing Cybercrime Regulation on a Global Level', JIST (2012) 67.

1.1 Casey, E 'Digital evidence and computer crime: Forensic science, computers and the internet' (2nd edition) (2004).
1.2 Leslie, D '*Legal Principles for Combatting Cyber-Laundering'* (2014).
1.3 Papadopoulos, S; S, Snail, 'Cyber@ law SA' (3rd edition) (2012).
1.4 Snyman C 'Criminal Law' (5th edition) (2002).
1.5 Snyman C 'Criminal Law' (6th edition) (2008).
1.6 Tapper, C 'Computer Law' (1990).
1.7 Van Der Merwe, D; Roos A; Pistorius T; Elselen S (1st edition) (2008) '*Information and Communications Technology law'.*
1.8 *Van Der Merwe, D, Roos, A; Pistorius T; Elselen S; Nel S 'Information Communication and technology law' (2nd edition) (2016).*

2. South African Case Law:

2.1. *S v Cwele and Another* 2013 (1) SACR 478 (SCA).
2.2. *S v Douvenga* District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003, unreported.
2.3. *S v Howard* (unreported case no 41/258/02, Johannesburg Regional Magistrates Court).
2.4. *S v Kidsonn* 1991 (1) SACR 33 (W).
2.5. *S v Naidoo* 1998 (1) BCLR 46 (D).
2.6. *S v Van den Berg* 1991 (1) SACR 104 (T).

3. Foreign Case Law:

3.1. *US v Council Court of Appeals* no 131083 (2005).
3.2. *US v Czubinsla* 1069 (1997).

4. Journal Articles:

4.1. Barker G, 'Trespassers will be prosecuted: Computer crime in the 1990's (1993) *Computer law Journal* volume 1.

4.2. Broadhurst, R 'Developments in the global Law Enforcement of Cyber-crime', Policing: An International Journal of Police Strategies & Management (2006) Volume 29.

4.3. Cassim, F 'Formulating Specialised Legislation to Address the Growing Spectre of Cyber Crimes: A Comparative Study' (2009) *Potchefstroom Electronic Law Journal* Volume 12.

4.4. Cassim, F 'Addressing the Spectre of Terrorism: A Comparative Perspective' (2012) *Potchefstroom Electronic Law Journal* volume 15.

4.5. Cassim, F "Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?" (2015) 18 *Potchefstroom Electronic Law Journal* Volume 2.

4.6. Coetzee J 'the Electronic Communications and Transactions Act 25 0f 2002: Facilitating Electronic Commerce.' (2004) *Stellenbosch Law Report*.

4.7. Kufa, M 'Cybersurfing without boundaries: The relationship between evidence and computer crimes" De Rebus December 2008.

4.8. Grobler, M; Van Vuuren, J; Zaaiman, J 'Preparing South Africa for Cyber Crime and Cyber Defence' (2013) *Systematics, cybermetics and informatics*.

4.9. Snail, S 'Cybercrime in the context of the ECT Act' (2008) *Juta's Business Law*.

4.10. S. Snail 'Cybercrime in South Africa- Hacking, Cracking and Other Unlawful Online Acts' (2009) *Journal of information, law and technology* volume 1.

4.11. Snail, 'The African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.' 2011.

4.12. Van Der Merwe, D 'Computer crime- Recent national and international Developments' (2003) *Tydskrif vir die Hedendaagse Romeins-Hollandse Reg V*olume 66.

4.13. Watney, M 'The Evolution of Legal Regulation of the Internet to Address Terrorism and Other Crimes' (2007) *Tydskrif vir die Suid-Afrikaanse Reg* volume 3.

4.14. Watney, M 'The way forward in addressing cybercrime regulation on a global level'i (2012) *Journal of Internet Technology and Secured Transactions*.

5. International Law Instrument:

5.1. African Union Convention on the Establishment of a Credible Legal Framework for Cyber security in Africa.

5.2. Colorado Computer Crime Act of 1973.

5.3. Council of Europe's Convention on Cyber Crime, Budapest, 23 XI.2001.
5.4. Counterfeit Access device and Computer Fraud and Abuse Act of 1984.
5.5. Electronic Communications Privacy Act of 1986.
5.6. USA Patriot Act of 2001.

6. South African Law Legislation:

6.1. Electronic Communications and Transactions Act, Act 25 of 2002.
6.2. Financial Intelligence Centre Act, Act 38 of 2001, herein after referred to as 'FICA'.
6.3. Prevention of Organised Crime Act, Act 38 of 1999.
6.4. Regulation of Interception of Communications and Provision of Communications-Related Information Act, Act 70 of 2002.

7. Draft Legislation:

7.1. Cyber Security Act of 2012.
7.2. Former Vice President Protection Act.
7.3. Proposed Bill on Cyber Crimes and Cybersecurity and Related Matters Bill 2015

8. On-line Resources:

8.1. Bawa N, 'The regulation of the Interception of Communications and provision of Communication relation information Act' www.thornton.co.za (accessed 15 July 2016).
8.2. Bernstan, Ebrahim, Obane 'Concerns raised over SA cybersecurity law' www.news24.com (accessed 20 October 2015).
8.3. Comments by the Law Society of South Africa on the Cyber Crimes and Cybersecurity Bill', www.lssa.org.za (accessed 30 April 2016).
8.4. Consultation document on Cyber Crimes and Cybersecurity Bill, www.justice.gov.za (accessed 20 October 2015).
8.5. Duncan 'A new Bill threatens our digital rights and raises the spectre of internet censorship', www.mailandguardian.co.za (accessed 16 October 2015).

8.6. Newmark, 'Boston US indicts hackers in biggest cyber fraud case in history' www.reuters.com (accessed 25 May 2016).

8.7. Right2Know campaign: 'Legislation: Concerns over proposed cyber law', www.Right2knoww.org.za (accessed 20 October 2015).

8.8. Right2Know campaign: 'What's wrong with the Cyber Crimes Bill-The seven deadly sins', www.Right2know.org.za (accessed 30 November 2015).

8.9. Tshongweni, M, 'Concerns Raised over Cybercrime and Cybersecurity Bill is SA' www.itnewsafrica.com (accessed 22 September 2015).

9. Other:

9.1. Gordon. G 'The hidden economy of Cyber-crime.', Sunday Times- 12 February 2012.

9.2. Snail. S 'Cybercrime and cybersecurity legislation in Africa- with an emphasis on cyber terrorism and cyberwarfare from a South African perspective' Document presented at the *Lex Informatica* 8 July 2016.

9.3. Snail. S 'Cybercrime in South Africa and international perspectives' – presentation at *Lex Informatica* in Pretoria 8 July 2016.

9.4. Watney M 'Cybercrime Regulation at a Cross-Road: State and Transnational laws versus Global Laws', International Conference on Information Society, 2012.

10. Thesis

10.1. Maat. S 'Cybercrime: 'A Comparative Law Analysis', unpublished LLM Dissertation, University of South Africa (2009).

10.2. Sulfab. M, 'Challenges of Cybercrime in South Africa' American Military University (2004).