

https://dspace.org/

The effectiveness of detection and prosecution of cybercrime threats against companies in South Africa

Naidoo, Shanine

2023
niversity of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/38631
Naidoo, Shanine. (2023). The role of design houses [Master's dissertation, University of the Witwatersrand, Johannesburg]. WireDSpace. https://hdl.handle.net/10539/38631

Downloaded from a DSpace repository. https://dspace.org/

THE EFFECTIVENESS OF DETECTION AND PROSECUTION OF CYBERCRIME THREATS AGAINST COMPANIES IN SOUTH AFRICA

by

803184

Submitted in partial fulfilment of the requirements for the degree of
Master of Laws by Coursework and Research Report
at the University of the Witwatersrand, Johannesburg

Date: 6th March 2023.

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG | WITS SCHOOL OF LAW

LLM BY COURSEWORK AND RESEARCH REPORT

PLAGIARISM DECLARATION

(For Research Reports)

Surname: __NAIDOO_____ First name ___SHANINE_____

Student No: _____803184_____

Course Code:

L	A	W	S	7	1	8		A

Course Name: _Research Report (F/T)/ Research Report **Part I**/ Research Report **Part II** (Circle the correct option)

Supervisor: _____ALINA STAROSTA_____

Research Title: **THE EFFECTIVENESS OF DETECTION AND PROSECUTION OF CYBERCRIME THREATS AGAINST COMPANIES IN SOUTH AFRICA**

I certify that the word count of this submission is _____10362_____**words** (including footnotes, but excluding the bibliography). **KINDLY NOTE THAT THE MAXIMUM WORD COUNT IS 10 500 WORDS**.

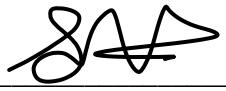
Plagiarism is the **"failure to acknowledge the ideas or writing of another"** or **"presentation of the ideas or writing of another as one's own"** and should be read to cover intentional and unintentional failure to acknowledge the ideas of others. In this context "others" means any other person including a student, academic, professional, published author or other resource such as the internet.

The University of the Witwatersrand, Johannesburg believes that failing to acknowledge the use of ideas of others constitutes an important breach of the values and conventions of the academic enterprise. It has therefore been resolved that all students should be required to sign a declaration that they are aware that they are required to submit their own unaided work and that plagiarism is unacceptable.

I declare the following:

a) I am aware that plagiarism (the use of someone else's work without their permission and or without acknowledging the original source) is wrong;

b) I am aware that any work that I submit for assessment must be my own unaided work except where I have explicitly indicated otherwise;
c) I am aware that I must follow the required conventions in referencing the thoughts and ideas of others;
d) I understand that the University of the Witwatersrand may take disciplinary action against me if I do not submit my own unaided work or if I fail to acknowledge the ideas or words of someone else in my writing and that lecturers are obliged to report incidents of plagiarism to the Plagiarism Committee of the School of Law;
e) I have been provided with a copy of the Senate Policy on Plagiarism which is also available from LB41 or on http://www.wits.ac.za/depts/wcs/helpdesk/PLAGIARISM%20POLICY.doc I have read and understood the above plagiarism declaration and confirm that the work submitted is entirely my own except where otherwise acknowledged.

Signature:  Date: ____06 March 2023_____

Notes (please read very carefully): · This sheet must be used as a cover page for ALL assignments in the School of Law. You are required to present a 2nd copy of your assignment for stamping in room LB13, which copy (once stamped) you will keep as your proof that you have handed in the assignment. A percentage of your mark will be deducted for every day (or part thereof) that an assignment is late.

ABSTRACT

The rise of digital technology has brought about many benefits to modern society. However, this advancement has also led to an increase in cybercrime activities, which has become a significant threat to individuals and organizations worldwide. In South Africa, cybercrime attacks against companies have become increasingly rampant, posing significant risks to their operations and even their existence. As a result, there is a growing concern about the effectiveness of the measures put in place to detect and prosecute cybercrime threats against companies. The purpose of this report is to investigate the efficiency of detecting and prosecuting cybercrime attacks against South African companies. While the term "cybercrime" encompasses a broad range of activities, this research will focus primarily on evaluating cybercrime threats that specifically target companies and their cybersecurity. The reason for this is that such attacks can have dire consequences on companies' operations and existence, ranging from financial losses to reputational damage. To achieve this objective, the study will pursue a twofold approach. Firstly, it will evaluate the effectiveness of South Africa's legislation in detecting and prosecuting cybercrime threats against companies. This includes a comprehensive examination of the legal frameworks and policies currently in place to combat cybercrime activities in the commercial sphere. Secondly, it will evaluate whether companies can rely on law enforcement agencies in South Africa to provide adequate protection against such threats. This will involve a critical analysis of the capacity and capability of law enforcement agencies to respond to cybercrime attacks against companies. The findings of this report will contribute significantly to the understanding of the effectiveness of detecting and prosecuting cybercrime attacks against South African companies. The recommendations made will provide valuable insights into how to improve the detection and prosecution of cybercrime threats in the commercial sphere. This study will be beneficial to policymakers, law enforcement agencies, and companies operating in South Africa, as it will help to enhance their understanding of the threats posed by cybercrime and the measures needed to mitigate them.

TABLE OF CONTENTS

DECLARATION..... 1

ABSTRACT..... 3

1. INTRODUCTION..... 5

2. OVERVIEW OF CYBER LAW AND TYPES OF CYBERCRIME THREATS AGAINST
   COMPANIES:.....10

3. SOUTH AFRICAN LAW RELATING TO THE DETECTION AND PROSECUTION OF CYBERCRIME
   THREATS..... 16

4. SHORTCOMINGS IDENTIFIED
   24

5. RECOMMENDATIONS
   ……..... 31

6. CONCLUSION
   ……..... 36

BIBLIOGRAPHY..... 38

CHAPTER 1: INTRODUCTION

In the age of digitization, the world has become globally connected.[1] Cyberspace provides commercial players a platform to execute business with other commercial players on a global scale, in an inexpensive manner.[2] Unfortunately, this exciting cyber era has also negatively impacted society.[3] For the opportunistic, global digital accessibility offers new possibilities for crime.[4] Businesses and individuals alike lose millions to computer-savvy fraudsters.[5] For example, computer networks may be used to capture confidential information, like trade secrets, and disrupt computer systems, threatening companies' success.[6]

Law enforcement has fallen behind due to the lack of resources and necessary skills needed to combat the ever-evolving danger, aptly labeled as *cybercrime*.[7] Existing laws do not adequately protect against cybercrimes being perpetrated and new legislation is still trying to catch up to practical realities with very few judicial precedents for direction.[8]

Defining Cybercrime:

Cybercrime, sometimes known as "computer crime", lacks a definite definition.[9] According to Wasik,[10] cybercrime is a broad issue, making it difficult to agree on specific terminology.[11] Chen, warns that uncertainty over a definition of cybercrime may lead to confusion when determining if one is dealing with cybercrime, impeding the creation of effective and consistent solutions to cybercrime problems.[12]

---

[1] Cross M *Scene of the Cybercrime* 2nd ed (2008) 725 at 2.
[2] Ibid.
[3] Cross op cit note 1 at 2.
[4] Rudner Martin 'Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge' (2013) 26 *International Journal of Intelligence and Counterintelligence* 453- 481 at 454.
[5] Ibid.
[6] Rudner op cit note 4 at 454.
[7] Ibid at 455.
[8] Cross op cit note 1 at 3.
[9] Ibid.
[10] Wasik, M 'Crime and the Computer' (1991) *Oxford: Clarendon Press* 159-160 at 159.
[11] Cassim F 'Formulating Specialized Legislation to Address the Growing Specter of Cybercrime: A Comparative Study' (2009) 12(4) *PER* 360 at 39.
[12] Chen, C D 'Computer crime and the Computer Fraud and Abuse Act of 1986' (1990) 10(1) *Computer Law Journal* 71-86 at 72.

Cybercrimes are different to traditional crimes because these crimes are committed with a click of a button.[13] Cybercrimes include the use of fewer resources, and can be perpetrated in any jurisdiction.[14]

In 2004, the Council of Europe ('CoE') defined cybercrime as "any unlawful, unethical, or unpermitted data processing and/or transfer activity".[15] According to Sieber, this definition proves to be problematic because it is too wide.[16] This author is of the opinion that Sieber accurately describes the definition as too wide because 'unethical behavior' does not always imply the commission of criminal conduct punishable by law.[17]

Academic scholars in South Africa have attempted to define cybercrime. Burchell[18] underlines the need to distinguish cases in which computers are the subject of a crime and those which computers are the mechanism used to perpetrate the crime.[19] Burchell expresses the opinion that using a computer to conduct a crime is not any different than using a weapon to kill, and if a computer is only used as a tool to commit a crime, conventional criminal law should apply.[20] In the opinion of this author, this definition is problematic because whether or not the crime was committed with the aid of a computer, the fact that a computer plays an *active role*[21] in the criminal offence, should qualify as a cybercrime.[22] Prosecution of a cybercrime specifically, rather than the offending conduct as a crime in general, has several advantages.[23] First, cybercrimes are often complex and involve the use of advanced technology, which may require specialized knowledge and expertise to investigate and prosecute.[24] By specifically criminalizing cybercrimes, law enforcement agencies are better equipped to investigate and prosecute these offenses, as they can focus their resources and expertise on these specific types

[13] Cassim op cit note 11 at 39.
[14] Ibid.
[15] Organization for Economic Co-operation and Development, 2004.
[16] U. Sieber 'New Legislative Responses to Computer-related economic crisis' (1986) 76 *The International Emergence of Criminal Information Law* 5 at 23.
[17] Ibid.
[18] Burchell J 'Criminal Justice at the Crossroads' (2002) 19 *SALJ* at 585.
[19] Ibid.
[20] Burchell op cit note 18 at 586.
[21] Kader S and Minnar A 'Cybercrime investigations: Cyber-process for detecting of cybercriminal activities, cyber-intelligence and evidence gathering' 5 (2015) *Acta Criminologica: SAJC* 124- 134 at 127.
[22] Ibid.
[23] Salter, M R. and Van Erp, J M 'Prosecuting Cybercrime: An international Perspective' 1 (2021) *International Journal of Cybersecurity Intelligence and Cybercrime* 47- 61 at 50-54.
[24] Ibid.

of crimes.[25] Additionally, legislatures are allowed the ability to provide specific penalties for cybercrime offenses, which take into account the unique nature of these offenses and the potential harm they can cause.[26] By having specific penalties for cybercrimes, it sends a clear message that these offenses are taken seriously and will not be tolerated, which can act as a deterrent to potential offenders.[27]

Watney[28] defines cybercrime as:

> "Cybercrime includes any unlawful acts in which a computer, computer system, information network, or data is the objective of the crime, as well as known illegal activities or crimes performed actively through or with the assistance of computers, computer systems, information networks, or data".[29]

This definition, in the authors opinion, is the most useful guideline for defining cybercrime as 'information technology crime'. The definition encompasses any criminal conduct involving a computer system, regardless of whether the computer is the tool used to accomplish the crime.[30] The focus of cybercrime has shifted to data and information technology.[31] The above definition encapsulates the nature of cybercrimes and is wide enough to allow for future cybercrimes to fall within its ambit.[32] Furthermore, this definition accommodates the technology aspect of the offence and the elements of the crime.[33]

1.1 Articulating the problem:

> "Throughout history, law has struggled to keep pace with social, cultural, economic and technological change".[34]

---

[25] Salter op cit note 23 at 50-54.
[26] Brenner, S W 'Prosecuting Cybercrime: Challenges and Solutions' 97 (2007) *Journal of Criminal Law and Criminology* 1361-1395 at 1370-1375.
[27] Ibid.
[28] Watney M M 'Die strfregtelike en prosedurele middele ter bekamping van kubermisdaad' (deel 1) (2003) *TSAR* 56 at 10.
[29] Ibid.
[30] Watney op cit note 28 at 10.
[31] Ibid.
[32] Dumchikov, M, Fomenko, A, Yunin, O, Pakhomov, V & Kabenok, Y 'The essence and classification of cybercrime in the field of computer information' 11(51) (2022) *Revista Amazonia Investiga* 291-299 at 292.
[33] Ibid.
[34] Arkin et al 'Prevention and Prosecution of Computer and high technology crime' (1990) 1 at 1.

This report is concerned with the efficiency of detecting and prosecuting cybercrime attacks against South African companies. The term ‘cybercrimes’ is very broad, and this report will only focus on assessing cybercrime threats that target companies and threaten companies’ cybersecurity which has dire consequences for companies’ operations and existence. This report seeks to evaluate, first, whether South Africa’s legislation governing detection and prosecution of cybercrime threats is effective, and second, whether companies can rely on South African law enforcement for adequate protection against cybercrime threats. Thereafter, recommendations will be made to contribute to the effective detection and prosecution of cybercrime threats in the commercial sphere.

1.2 Structure and Overview

Chapter 1 served the purpose of providing an introduction to this report by looking at the definitions of cybercrime and articulating the problem statement of this paper.

Chapter two provides an overview of cyber law. The chapter also discusses the types of cybercrime threats against companies such as phishing, SQLI, and malware. It highlights the potential consequences of these threats, including the cessation of a company's production and putting companies at the mercy of attackers who manipulate company owners into meeting excessive demands. Therefore, the development of legislation and regulation in this regard is imperative. Finally, the chapter provides a general overview of cyber law in South Africa and its development over time, highlighting the legislative journey in the country, beginning with the Promotion of Access to Information Act 2 of 2000 till the Cybercrimes Act 19 of 2020.

Chapter 3 aims to provide an overview of South African law in relation to the detection and prosecution of cybercrime threats. Specifically, it will examine the Cybercrimes Act 19 of 2020 and evaluate its effectiveness in criminalizing cybercrime threats such as phishing, malware, and SQLI. To achieve this, certain sections of the Act will be highlighted and assessed. In addition, the chapter will analyze the detection and prosecution procedures outlined in the Act, including the strategies, investigative units, and courts used to adjudicate cybercrimes in South Africa.

Chapter 4 evaluates the shortcomings in the provisions outlined in the previous chapter by highlighting the shortcomings that exist in the current legal framework in South Africa, particularly when it comes to dealing with cyber threats. The chapter analyses the strategies

that are in place to address cyber threats, such as detection and prosecution strategies. Another significant issue that is addressed in this chapter is the lack of requisite skills in South Africa to deal with cyber threats effectively. Additionally, the chapter evaluates the major obligation that is placed on companies in South Africa to ensure the security of their networks and data. The effectiveness of this obligation is analysed.

Chapter 5 presents suggestions for improvement through an examination of academic literature and the authors own research efforts. Specifically, the chapter deals with a recommendation on how the investigative units may run more efficiently. Additionally, the author provides an avenue for the attainment of requisite skills in South Africa, how companies can handle the major obligations that are placed on them via the Cybercrimes Act and the final recommendation is for an establishment of statutory SCCCs.

In Chapter 6, this report will draw together the findings from the previous chapters and offer a comprehensive conclusion. This chapter will recapitulate the key themes, arguments, and insights presented in each chapter and synthesize them into a cohesive whole.

CHAPTER 2: AN OVERVIEW OF CYBER LAW AND TYPES OF CYBERCRIME THREATS AGAINST COMPANIES

2.1 Overview of Cyber law:

Cyber law, like cybercrime, has no precise definition.[35] Cyber law is a new branch of law dealing with legal concerns that arise from the usage of the internet and other digital technologies.[36] It covers a wide variety of legal issues, including data protection and privacy, cybercrime, intellectual property, e-commerce, and telecommunications.[37] Keeping up with the fast-expanding technological world is one of the most difficult tasks in cyber law.[38] When new technologies arise, so do new legal difficulties and challenges that necessitate creative legal responses.[39]

Cybercrime, inter alia, is one of the key focus areas within cyber law.[40] Cybercrime can be characterized as an illegal activity performed via the use of computer networks or the internet.[41] Structured Query Language Injection, Phishing, and Malware are a few examples of the imminent threats in cyberspace which will be discussed in more detail below. Cyber law addresses these challenges by establishing legal frameworks for investigating, prosecuting, and punishing cyber offenders.[42] Cyber law does so by encompassing the legal concerns surrounding the use of networked information devices and technology for communicative, transactional, and distributive purposes.[43]

When the Internet was first conceived, its use for unlawful and immoral acts was not contemplated.[44] Due to the anonymity of the internet, anybody may engage in a range of illicit actions without consequence.[45] Individuals are taking advantage of "grey zones" to engage in criminal activity in cyberspace, thus necessitating the need for regulation.[46] Attacks against companies, for example, are one of these grey zones.[47] Given the lack of legislation in this area, as well as the difficulties in detecting and prosecuting such cybercrimes against

[35] Chauhan A 'Evolution and Development of Cyberlaw – A Study with Special reference to India' (2013) *SSRN* 1-18 at 2-3.
[36] Lessig L 'The Law of the horse: What cyberlaw might teach' (1999) 113 *Harvard Law Review* 501-549 at 510.
[37] Brian, C 'Cyberlaw: The Law of the Internet and Information Technology' (2020) *Pearson Education* 1-288 at 20-23.
[38] Ibid.
[39] Brownsword, R., Goodwin, M., & Johnston, A 'Law and the Technologies of the Twenty-First Century: Text and Materials' (2012) *Cambridge University Press* 453 at 1-3.
[40] Gordon, F., McGovern, A., Thompson, C., and Wood, M. A 'Beyond cybercrime: New Perspectives on crime, and digital technologies' 11(1) (2022) *International Journal for Crime, Justice and Social Democracy. Brisbane, Queensland, Australia: Queensland University of Technology.* 1-8 at 1-2.
[41] Ibid.
[42] Gordon op cit note 40 at 2.
[43] Chauhan op cit note 35 at 2-3.
[44] Ibid.
[45] Chauhan op cit note 35 at 2-3.
[46] Ibid.
[47] Holt, T. J., & Bossler, A.M 'Cybercrime and Digital Forensics: An introduction' (2015) *Routledge* 1-812 at 14.

companies, cyber criminals prey on companies, which can have serious economic implications.[48]

2.2 Types of cybercrime threats against companies:

Phishing was the first danger to companies in the 1990s.[49] Phishing is an attack in which the hacker disguises himself as a reputable person or organization to deceive potential victims into revealing sensitive information or paying money.[50] Spear phishing, which is type of phishing, targets businesses in particular.[51] The hackers explore the Internet for studied facts about a target's employees, identities and professional relationships of significant individuals in their firms.[52]

The hacker uses this information to craft a convincing email masquerading as an executive in the organization, ordering employees to submit a substantial payment to either the executive or a corporate supplier, while the fraudulent money transfer link delivers to the attacker.[53]

In 1998, the threat of Structured Query Language Injection ("SQLI") began to emerge.[54] SQLI is a cyber-attack in which hackers use software faults in online applications to steal, destroy, or change data.[55] A hacker uses SQLI code to disrupt a data base and obtain control of a website or information systems used by businesses to store data.[56]

SQLI is risky because hackers can acquire the confidential information of millions of users in a single SQLI attack.[57] Cybercriminals sell this personal information on the dark web, where

[48] Ibid.
[49] Markus J 'The rising threat of launchpad attacks' (2019) 17(5) *IEEE Security & Privacy* 68-72 at 68-69.
[50] Dhamija, R, Tygar, D and Hearst, M 'Why phishing works' (2006) *Proceedings of the SIGCHI conference on Human Factors in computing systems* 581-590 at 584.
[51] Ibid.
[52] Sarfraz M 'Cybersecurity Threats with New Perspectives' ed (2021) *intechopen* 178 at 110.
[53] Dhamija, et al op cit note 16 at 584.
[54] Aggarwal, P, et al. 'Random Decision Forest approach for Mitigating SQL Injection Attacks' (2021) *International Conference on Electronics, Computing and Communication* 1-5 at 1.
[55] Halfond W, Viegas, J and Orso, A 'A classification of SQL-injection attacks and countermeasures' (2006) 1 *In Proceedings of the IEEE international symposium on secure software engineering* 13-15 at 14.
[56] Ibid.
[57] Singh N & Tiwari P 'SQL Injection Attacks, Detection Techniques on Web Application Databases. In Rising Threats in Expert Applications and Solutions: Proceedings of FICR-TEAS. (2022) *Singapore: Springer Nature Singapore* 387-394 at 389.

it can be utilized for a variety of illicit reasons.[58] This leads to identity theft, a cybercrime in which a criminal acquires entry to a person's private information in order to steal money, open a phone/internet account in your name, arrange a criminal action in your name, and seek for government benefits in your name.[59]

In 2002, the threat of Malware began.[60] Malware, sometimes known as "malicious software" is a catch-all phrase for any malicious program or code that is damaging to systems.[61] The Internet and email are the two most popular methods for malware to get access to computers.[62] A Trojan horse is one of the most destructive forms of malware.[63] In order to deceive the user, it frequently disguises itself as something beneficial.[64] Once installed, the Trojan allows the attackers behind it to obtain unauthorized access to the infected machine.[65] Trojans can then be used to steal financial information or install other types of malware, most often ransomware.[66]

Malware attacks result in the cybercrime of Ransomware.[67] This is when a company's information or the threat of data destruction is being held hostage.[68] The company is unable to access files, databases, or programs. As a result, the entire business is rendered inoperable.[69]

These threats' consequences can have long-term effects for companies.[70] The implementation of these threats might result in the cessation of a company's production and puts companies at the whim of attackers who manipulate company owners into meeting excessive demands.[71] Therefore, the development for legislation and regulation in this regard is imperative.

---

[58] Gokhale G 'Network analysis of dark web traffic through the geo location of South African IP address' (2020) *Smart cities performability cognition and security* 201-219 at 201.
[59] Ibid.
[60] Robert, L and Hamrock, J 'Using entropy analysis to find encrypted and packed malware' (2007) 5(2) *IEEE Security & Privacy* 40-45 at 40.
[61] Ulrich, B et al. 'Scalable, behavior-based malware clustering' (2009) 9 *NDSS* 8-11 at 8.
[62] Ibid.
[63] Ulrich op cit note 61 at 8.
[64] Ibid.
[65] Ulrich op cit note 61 at 8.
[66] Ibid.
[67] Ulrich op cit note 61 at 8.
[68] Ibid.
[69] Ulrich op cit note 61 at 8.
[70] Cashell B, et al. 'The Economic impact of cyber-attacks' (2004) 2 *Congressional research service documents, CRS RL32331 (Washington DC)* 1-41 at 15.
[71] Ibid.

2.3 General overview of Cyber law in South Africa and development over time:

The legislative journey in South Africa began in 2000.[72] The *Promotion of Access to Information Act 2 of 2000* ("PAIA")[73] is a component of South African law that supports transparency and accountability in the public and commercial sectors by allowing access to information.[74] This access to information applies to records in the public or private sectors.[75] The Act is founded on the constitutional right to information, which is stated in Section 32 of the Republic of South Africa's Constitution of 1996.[76]

While PAIA does not explicitly protect against cybercrime, it can be used to acquire information needed to investigate or prosecute cybercrime.[77] PAIA, for example, can be used to seek information from public bodies such as law enforcement or government departments that may be pertinent to a cybercrime inquiry.[78]

The *Electronic Communications Act 25 of 2002*[79] ("ECTA") is a critical piece of legislation that has had a major effect on the evolution of South African cyber law.[80] ECTA is a general-application legislation that governs transactions that are completed electronically or by data transmissions.[81] ECTA has created essential safeguards for people and companies working in the online world by providing a legal framework for the regulation of electronic communications. Chapter XIII of ECTA deals with cybercrime and controls unlawful access to, interception of, or tampering with data, which is relevant to data breaches.[82] Sections 85-88 established a range of cybercrime offenses.[83] ECTA had been widely criticized for being ineffective.[84] An example of one of the major criticism is towards the penalties for engaging

[72] Burchell 'Criminal Justice at the Crossroads' (2002) 119(3) *SALJ* 579-602 at 585.
[73] The *Promotion of Access to Information Act 2 of 2000 of South Africa.*
[74] Papadopoulos, S & Snail, S 'Cyberlaw @ SA III: The law of the internet in South Africa' (2012) 3 Van Schaik at 5-6.
[75] Ibid.
[76] Papadopoulos op cit note 74 at 5-6.
[77] Papadopoulos S & Snail ka Mtuze S 'Cyberlaw @ SA The Law of the Internet in South Africa 4/e' 4th ed (2022) *Van Schaik Publishers* at chapter 1 para 1.2.2.
[78] Ibid.
[79] *The Electronic Communications and Transactions Act 25 of 2002 of South Africa*.
[80] Van der Merwe 'Information and Communications Technology Law' 3rd ed (2021) *LexisNexis* 795 at chapter 2 at para 2.4.
[81] Ibid.
[82] Supra note 79.
[83] Ibid.
[84] Van der Merwe op cit note 80 at chapter 2.

in cybercrime, as defined in section 89 of ECTA, are deemed to be insufficiently severe.[85] It is maintained that these sanctions are insufficient deterrents to prevent cybercrime, and that ECTA should be changed to incorporate more severe penalties.[86] While the ECTA is a crucial piece of legislation that provides a legal foundation for combating cybercrime in South Africa, some areas needed to be revised and improved in order to better handle new and growing cybersecurity threats.[87]

Following ECTA, the *Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002* ("RICA")[88] came into effect and has made a major contribution to the development of South African cyber law.[89] RICA protects privacy by enabling state officials to intercept communications under specified processes and safeguards.[90] RICA has contributed to the development of cyber law in South Africa by clarifying the government's powers to intercept communications and the boundaries of those powers in the context of fundamental rights to privacy and free speech.[91]

Protection of Personal Information Act 4 of 2013 ("POPI") made a major contribution to the growth of South African cyber law by introducing a complete framework for the protection of personal information in the digital realm.[92] POPI Act covers this void by setting principles and requirements for the legal handling of personal data both online and offline.[93] The POPI Act makes an important addition to the development of cyber law in South Africa by providing a legislative framework for protecting personal information in the digital realm.[94] This framework gives people more control over their confidential information.[95] Furthermore, it provides organizations with clear guidelines on how to legally manage personal information, lowering the risk of cybercrime and privacy violations.[96]

---

[85] Cassim, F 'Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players' 44 (1) (2011) *The Comparative and International Law Journal of Southern Africa* 123-138 at 129- 134.
[86] Ibid.
[87] Cassim op cit note 85 at 129-134.
[88] Ibid.
[89] Papadopoulos op cit note 77 at chapter 13.
[90] Ibid.
[91] Papadopoulos op cit note 77 at chapter 13.
[92] Van der Merwe op cit note 80 at chapter 2.
[93] Ibid.
[94] Ramluckan, T 'International Humanitarian Law and its Applicability to the South African Cyber Environment' 19(3) (2020) *Journal of Information Warfare* 102-117 at 106-107.
[95] Ibid.
[96] Ramluckan op cit note 94 at 107.

South Africa's most recent development in cyber law is the *Cybercrimes Act 19 of 2020* ("the Act").[97] The Act includes thorough and up-to-date regulations that handle the present cybercrime landscape.[98] The Act has additional cybercrime charges such as harassment, malware dissemination, cyber forgery, and online identity theft that were not previously covered by the ECTA.[99] This has resulted in a more robust legal structure for prosecuting cybercriminals and safeguarding people and companies against online threats.[100]

Chapter three will focus on key areas of the Cybercrime Act, specifically its effectiveness in detecting and prosecuting cybercrime. Effective detection is crucial as companies often don't realize they are under attack by cybercriminals.[101] Effective prosecution is also important to hold lawbreakers accountable and discourage future crimes.[102] If these aspects are not effective, they must be brought in line with their intended purposes.[103]

CHAPTER 3: SOUTH AFRICAN LAW RELATING TO THE DETECTION AND PROSECUTION OF CYBERCRIME THREATS.

3.1 The Cybercrimes Act 19 of 2020:

The Cybercrimes Act is South Africa's existing legislation regulating cybercrime.[104] The Act will not be examined in its entirety, rather, the parts highlighted below are those that are

[97] The *Cybercrimes Act 19 of 2020 of South Africa.*
[98] Papadopoulos op cit note 77 at chapter 13.
[99] Ibid.
[100] Papadopoulos op cit note 77 at chapter 13.
[101] Gerstein, D.M 'Better Anticipating and Managing Today's Growing Cyber Risks' 7 (4) (2022) *The Cyber Defense Review* 15-30 at 27-30.
[102] Ibid.
[103] Gerstein op cit note 101 at 27-30.
[104] Supra note 97.

pertinent to cybercrime threats against companies. The inquiry will specifically look at whether the Act is effective in criminalizing cyber threats such as phishing, malware, and SQLI threats. Furthermore, this portion aims to determine the effectiveness of the detection and prosecution procedures.

The purpose of the Cybercrimes Act, according to the preamble, is to: "*To create offences which have a bearing on cybercrime; … to provide for the establishment of a designated Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations to report cybercrimes; to provide for capacity building; to provide that the Executive may enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes;…".*[105]

Chapter 2 of the Act deals with "*Cybercrimes, Malicious communications, sentencing and orders to protect complainants from the harmful effect of malicious communications".*[106] Part 1 of Section 2 creates new cybercrimes as criminal offenses. Section 3 criminalizes the unlawful acquisition of data and provides that *any person who unlawfully and intentionally accesses or intercepts any data, computer program, or system, with the intent to acquire information that they are not authorized to obtain, is guilty of an offense*.[107]

Subsections 3 (1)(a) and (b) of the section seek to punish the methods used for which data can be obtained illegally, such as phishing.[108] Phishing involves unauthorized access to computer systems or data for fraudulent purposes.[109] Phishing is a cybercrime technique used by impersonating a trustworthy source to trick individuals into providing sensitive information.[110] This illegal conduct falls under Section 3(1) of the Cybercrimes Act as the attacker intentionally gains unauthorized access to victim's computer system or data with the intention of using it for fraudulent purposes.[111] Therefore, this section of the Act can be used to effectively prosecute individuals who engage in phishing activities.[112]

[105] Ibid.
[106] Supra note 97 at Chapter 2.
[107] Supra note 97 at Section 3.
[108] Supra note 97 at Section 3.
[109] Markus op cit note 49 at 584.
[110] Ibid.
[111] Supra note 97 at section 3.
[112] Markus op cit note 49 at 584.

Section 4 criminalizes unlawful acts in respect of software or hardware tools.[113] Section 4 states that *any person who unlawfully and intentionally alters or destroys any data, computer program, or system, or causes such an act to occur, is guilty of an offense*.[114] In simpler terms, the Act makes it illegal for anyone to deliberately alter or destroy computer data, programs, or systems without authorization or permission. If someone does commit such an act, they are committing an offense under this section of the Act.

In this section, the final objective of the crime is the main focus, such as serious crimes, like data interception or interference.[115] Malware offenders exploit the ability to connect computer networks; they are often not present at the crime site, all they need is to get past the security measures that safeguard the database, network, or computer equipment.[116] Malware is a danger that falls under the purview of sections 3 and 4.

Malware results in the serious crime of ransomware.[117] Section 5 criminalizes unlawful interference with data or computer program in that *any person who unlawfully and intentionally interferes with or obstructs data, a computer program or system, with the intent to hinder or interfere with its functioning, is guilty of an offense*.[118] Ransomware is a type of malware that encrypts the victim's computer data and demands a ransom payment in exchange for the decryption key, which is an offense under this section of the Cybercrimes Act.[119]

Additionally, the conduct of SQLI also falls within the ambit of section 5.[120] Section 5 of the Cybercrimes Act criminalizes tampering with data or a computer program.[121] The element of an individual who unlawfully and willfully intercepts data from a computer device, network, or a national essential information structure must be satisfied for the activity to constitute a crime.[122] The provision is wide in its discretion of which devices may apply which is

[113] Supra note 97 at Section 4.
[114] Ibid.
[115] Supra note 97 at Section 4.
[116] Ibid.
[117] Ulrich op cit note 61 at 8.
[118] Supra note 97 at section 5.
[119] Alenezi M. N, Alabdulrazzaq H, Alshaher A & Alkharang M.M 'Evolution of malware threats and techniques: A review' 12 (3) (2020) *International Journal of communication networks and information security* 326-337 at 329.
[120] Ibid.
[121] Supra note 97 at section 5.
[122] Aggarwal op cit note 54 at 1.

commendable as the provision attempts to be all-inclusive of the instruments that can be used to interfere with data.[123]

The criminalization of SQLI is to protect the integrity, privacy, and confidentiality of data within a computer device.[124] Unlawful access permits the criminal to take additional steps to illegally get data.[125]

The above-mentioned sections highlight the fact that these threats, if materialized, are adequately criminalized by the Act and allow for prosecution. However, the Act contains an additional section to cover the event of the cyber threat not materializing.[126] Section 10 criminalizes the offence of cyber extortion and provides that:

> ***10. "Any person who unlawfully and intentionally—***
> *(a) threatens to commit any offence; or*
> *(b) commits any offence,*
> *contemplated in sections 3(1), 5(1), 6(1) or 7(1)(a) or (d), for the purpose of—*
> *(i) obtaining any advantage from another person; or*
> *(ii) compelling another person to perform or to abstain from performing any act, is guilty of the offence of cyber extortion".*[127]

The provision criminalizes the threat and/ or the actual commission of an offence for the purposes of obtaining any advantage of another person.[128] If any of these means are used to obtain any advantage from another person, then such an offence is punishable under this provision and constitutes the offence of cyber extortion.[129]

3.2 Procedural provisions, strategies, and investigative units:

[123] Papadopoulos op cit note 77 at chapter 1.
[124] Lakshmi, P.V.S 'SQL Injection detection analysis using deep learning' 8 (2022) *Journal of Engineering Sciences* 13 at 1-3.
[125] Manhas, S 'An Interpretive Saga of SQL Injection Attacks- Emerging Technologies in Data mining and information security' 1 (2022) *Proceedings of IEMIS, Singapore: Springer Nature Singapore* 1-3 at 1-3.
[126] Supra note 97 at section 10.
[127] Ibid.
[128] S Mabunda 'Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill' (2018) *Statute Law Review* 9. doi:10.1093/slr/hmx028.
[129] Supra note 97 at s10.

The Criminal Procedure Act serves as the legal foundation for search and seizure operations, therefore, it remains the starting point for all criminal investigations.[130] The purpose of the CPA is to regulate and control the manner in which law enforcement officials can carry out searches and seizures of property, including electronic devices and data, during criminal investigations.[131] The CPA sets out specific procedures that must be followed by law enforcement officials when conducting searches and seizures, including obtaining a search warrant from a magistrate or judge before conducting a search or seizure.[132] There are concerns that the CPA may not be sufficiently updated to address emerging issues related to digital technologies and electronic evidence.[133]

The Act, Chapter 5, gives police officers special procedural authority. [134] These provisions are intended to be utilized in conjunction with procedural procedures of Section 35 (1) of the CPA.[135] Section 35 (1) calls for the "return of any weapon, instrument, or other thing by means of which the offence in question was committed or was utilized in the commission of the same".[136] In circumstances where a laptop or computer is used to aid illegal behaviour, investigating authorities may take any 'device' used to facilitate the crime under Section 35 (1) of the CPA.[137]

The Act also allows for enhanced extraterritoriality jurisdiction.[138] Section 24 of the Act grants jurisdiction over crimes committed in other nations if such offenses have "effect in the republic".[139] Cybercrime is international with a multijurisdictional presence.[140] Thus, extradition is a critical instrument in the prosecution of cybercrime.[141] In addition to Chapter 2 of the International Co-operation in Criminal Matters Act of 1996, Chapter 6 of the Act allows for mutual help in the detection of cybercrimes and preservation of evidence.[142] It is critical to establish a framework to allow reciprocal cooperation between foreign authorities in the

[130] *Criminal Procedure Act 51 of 1977 of South Africa.*
[131] Basdeo, V 'The Constitutional Validity of Search and Seizure Powers in South African Criminal Procedure' 19 (2009) *PER/PELJ* 307-360 at 310-312.
[132] Ibid.
[133] Basdeo op cit note 131 at 310- 312.
[134] Supra note 97 at chapter 5.
[135] Supra note 130 at s35.
[136] Ibid.
[137] Supra note 130 at s35.
[138] Supra note 97 at s24.
[139] Ibid.
[140] Plachta, M & Zagaris, B 'Economic Sanctions' 38 (2022) *IELR* 291 at 12.
[141] Ibid.
[142] International Co-operation in Criminal Matters Act of 1996.

detection and prosecution of cybercrimes.[143] Given the internet and the multijurisdictional nature of cybercrime, global investigating authorities' strategic and joint efforts are critical to the effective prosecution of offenses.[144]

In addition to 'mutual assistance', chapter 6 of the Act introduces the 'Designated point of Contact', also known as the '24/7' point of contact clause.[145] It has not yet been legally constituted, but the Act mandates it be controlled by a cabinet member who is responsible for procuring workers, operating procedures, and maintenance plans.[146] The Cabinet member must be a police officer with experience and technical knowledge in cybercrime and cybersecurity.[147]

With regards to reporting cases to the Designated Point of Contact, it is deemed adequate to follow existing procedures.[148] As amended by the South African Police Service Amendment Act 10 of 2012, reporting must be made in the Directorate for Priority Crime Investigation (DPCI) in terms of section 34(1) of the Prevention of Organised Crime Act 12 of 2004 ("PoCA"). The Directorate Investigation offices can be contacted through email or fax number websites.[149]

The 24/7 point of contact clause is significant to address the difficulties of cross-border cybercrime since it is operational 24 hours a day, seven days a week.[150] The office is tasked with investigating cybercrimes that are major international concerns, and allows investigators to contact other countries in order to persuade international governments to cooperate with South African officials on issues of concern, particularly cybercrimes in which other countries have a similar or identical interest.[151]

To ensure the Designated Point of Contact clause is effective, the Act places an obligation on the Cabinet Member responsible for policing to ensure *there is sufficient and human and*

[143] Plachta op cit note 140 at 12.
[144] Ibid.
[145] Supra note 97 at chapter 6.
[146] Ibid.
[147] Supra note 97 at chapter 6.
[148] Khan, S, Saleh, T, Dorasamy, M, Khan, N, Leng, O & Vergara, R 'A systematic literature review on cybercrime legislation' 11 (2022) *F1000Research* 971 at 176.
[149] https://www.saps.gov.za/dpci/reportingguide.php.
[150] Supra note 97 at chapter 6.
[151] Ibid.

operation capacity to detect and prevent and investigate cybercrimes.[152] *To ensure the SAPS receives basic training relating to detecting and investigation and to develop and implement accredited training programmes for members of the SAPS.*[153] Computer or digital forensic professionals, in particular, are at the heart of the system for investigating and detecting cybercrimes.[154] Detecting and recovering evidence from websites and technological gadgets is a tough procedure that necessitates knowledge of information technology (IT) and computer forensics.[155] Any error, technological malfunction, biased intervention, or fabrication done at any level of an inquiry might impair the evidential value of the data gathered, rendering it inadmissible as evidence.[156]

The last point this report would like to draw attention to is that the Act places an obligation on Electronic Communications Service Provider ("ECSP").[157] Section 54 of the Act requires electronic communications service providers to "take reasonable steps to inform clients of cybercrime trends that may affect them; establish procedures for clients to report cybercrime; and inform clients of cybercrime prevention measures".[158]

Furthermore, if an electronic communications service provider discovers that its network is being used to commit cybercrime, it must promptly notify the National Cybercrime Centre and retain any information that will be useful in the detection of the cybercrime committed.[159] Failure to comply with the foregoing conditions will result in the service provider being charged with an offence and facing a fine of R10,000 for each day of non-compliance.[160]

After examining the Act in the context of cyberthreats, the Act is an effective piece of legislation that can be used effectively with regard to the detection and prosecution of cybercrime threats.

---

[152] Supra note 97 at s55.
[153] Ibid.
[154] Van Vuuren, J. J., Leenen, L,. & Pieterse, P 'Development and Implementation of Cybercrime Strategies in Africa with Specific Reference to South Africa' 19(3) (2020) *Journal of Information Warfare* 83-101 at 85-89.
[155] Ibid.
[156] Van Vuuren op cit note 154 at 85-89.
[157] Supra note 97 at s54.
[158] Ibid.
[159] Supra note 97 at s54.
[160] Ibid.

3.3 Prosecution of cyber threats in South Africa:

Article 22 of the CoE Convention governs the exercise of jurisdiction.[161] Section 90 of the ECTA reflects this, and section 24 of the Act expands on it. A detailed reading of the ECTA and the Act reveals that South Africa launched the Specialized Commercial Offences Court (SCCC) in 1999, with backing from Business Against Crime, to encourage a concentrated approach to the prosecution of commercial crimes in South Africa.[162]

SCCCs are not legally defined.[163] They are essentially the result of court specialization, which is one of the government's tactics for providing a number of accessible and service-oriented courts as well as "other judicial and quasi-judicial institutions" for all areas.[164] Based on this, the SCCC is a government plan to develop an environment in which human capabilities, management systems, and accessible infrastructure are more suited to particular concerns than in more generic court contexts.[165]

The Serious Commercial Crimes Unit (SCCU) prosecutes serious, complicated, and organized commercial crime in the SCCCs, which are dedicated courts on the regional court tier.[166] The SCCU is a business unit of the National Prosecuting Authority (NPA) tasked with prosecuting complex commercial crime cases originating from SAPS commercial branches.[167] The unit's clientele includes a diverse range of business complainants, ranging from private persons and corporations to governmental entities.[168] In general, the investigative technique is what is known as a 'prosecution-led investigation,' which comprises the prosecutor offering instructions on how the prosecution should be done as well as legal advice as needed along the process.[169]

[161] Velasco 2025 *ERA* Forum 7.
[162] The National Prosecuting Authority Annual Report 2018/2019 at 69.
[163] Ezeji, C. L., Olurola, A. A., & Bello, P. O. 'Cyber-related crime in South Africa: extent and perspective of state's roleplayers' 31(3) (2018) *African Journal of Criminology & Victimology'* 93-110 at 93-96.
[164] Ibid.
[165] Altbeker 2016 *Research Gate 31.*
[166] Ezeji op cit note 163.
[167] Ibid.
[168] Ezeji op cit note 163.
[169] Ibid.

At the end of 2019, the NPA has ten dedicated courts dispersed around the nation, with additional satellite offices in certain areas.[170] The SCCC technique is a prosecutor-guided investigation, in which prosecutors and the SAPS collaborate as a team, and the SAPS and courts are co-located to accelerate case resolution.[171] The prosecution's function during the investigative stage is to give legal advice. Cybercrime risks including commercial crime, in this author's perspective, were also supposed to come under the jurisdiction of the SCCCs.[172] Based on the Act, this author interprets cybercrime as a commercial crime, that is, a crime involving dishonesty that is designed to defraud a victim of his or her own property, which might be monetary in character.[173] As a result, since cybercrime risks like as phishing, malware, and SQLI, among others, are criminalized, they will be tried alongside other business crimes in the SCCCs.

The Cybercrimes Act can help detect and prosecute crimes against companies, but a lack of understanding among investigators and prosecutors may hinder its effectiveness. Chapter 4 will address these shortcomings. It's important to note that the Act is still new, so it's unclear how effective it is due to a lack of precedence.

CHAPTER 4: SHORTCOMINGS IDENTIFIED

4.1 The Cybercrime Act:

The previous chapter illustrated a detailed analysis of how certain cyber threats, such as phishing, malware, and SQLI are criminalized under chapter 2 of the Act. Furthermore, the Act goes a step further to make provision for an instance where these threats do not materialize, whereby the Act deems ‘cyber extortion’ as a criminal offence. In this aspect, the Act has done well. However, there are shortcomings identified of the Act. In this section, the problems identified with regard to the legislation are compared to the current status quo of South Africa.

[170] The National Prosecuting Authority Annual Report 2018/2019 at 69.
[171] Altbeker 2016 *Research Gate 31.*
[172] Ibid.
[173] Altbeker op cit note 171.

4.2 The shortcomings identified in the procedural provisions, strategies, and investigative units:

Concerning the establishment of investigative teams to combat cybercrime, the Designated Point of Contact section raises concerns. According to Sections 17B and 17D of the South African Police Service Act, 1995 as modified, the DPCI is tasked for combatting, investigating, and preventing national priority crimes such as major organized crime, serious commercial crime, and significant corruption.[174] This clause does not directly address cybercrime, but considering the commercial character of cybercrime conducted to defraud victims of their money, it is reasonable to presume that cybercrime is included in the definition of severe commercial crime in this provision.[175] According to the DPCI website, section 34 (1) of the Prevention and Combating of Corrupt Activities Act 12 of 2004 (PCCAA Act) requires any person in authority to report the offense to a police officer in the DPCI.[176] The PCCAA Act gives no mechanism for the average citizen to report to a police station.[177]

In terms of how commercial crime is being investigated in South Africa, the investigation is prosecution-led, with investigation teams comprised of prosecutors who give legal assistance and DPCI detectives.[178] However, Altbeker believes that instances should not be so serious that they warrant detection and prosecution by the Directorate of Special Operations, the forerunner of the DPCI.[179]

Furthermore, the Designated point of contact clause places the SAPS in charge of coordinating both domestic and international investigations, however, this seems to be overreaching for one agency to handle.[180] The idea to build a cybercrime reporting centre within the SAPS by the beginning of 2016 has fallen through.[181] The SAPS's annual performance plan for 2020-2021 aims to re-establish it as a component of the SAPS's medium-term planning.[182] This is

[174] Watney M 'Cybercrime and the investigation of cybercrime" in Papadopoulos S and Snail S (eds) *Cyberlaw@ SA III The Lay of the internet in South Africa* 3rd ed 333-350 (Van Schaik 2012).
[175] Ibid.
[176] Watney op cit note 174.
[177] Ibid.
[178] Watney M op cit note 174.
[179] Altbeker A "A model for justice delivery: The Specialized Commercial Crime Court" (2016) *Research gate* 31-34.
[180] Ibid.
[181] Watney op cit note 174.
[182] South African Police Service Annual Performance pka 2020/2021.

unfortunate since the reason cybercrimes are not reported to regular police is because society lacks trust in the police response.

Over the years, the SAPS has been widely chastised for its inefficiency.[183] This is primarily in response to the SAPS's overall poor performance and significant levels of police misbehaviour.[184] The SAPS annual reports portray a bleak image of diminishing efficacy, stating that contact crimes including murder, common assault, and robbery surged by 21% from 2020 to 2021, while commercial crime grew by 15% in the same period.[185] At the same time, the SAPS has been forced to pay more than R140 million in civil claims for behaviour by police officers between January and May 2021.[186] The public's trust in the SAPS has been eroded as a result of this irresponsible behaviour.[187]

Furthermore, the SAPS are understaffed and underfunded, which has made it difficult for the SAPS to deal with typical crimes.[188] Due to a major lack of skills and competence as a result of a lack of finances, it is difficult to determine how the SAPS would handle the designated point of contact if traditional crimes are not successfully controlled.[189]

4.3 Attainment of requisite skills:

Section 55 of the Act imposes a responsibility on the South African government to guarantee the creation of an operational capability to identify and investigate cybercrime.[190] Computer or digital forensic professionals, in particular, are at the heart of the system for investigating and detecting cybercrimes.[191] Years ago, it was recognized that an experienced team in the field of

[183] Johan Burger and Stuart Mbanyele 'Old Solutions won't fix South Africa's deteriorating police service' available at: https://issafrica.org/iss-today/old-solutions-wont-fix-south-africas-deteriorating-police-service accessed on 18 January 2022.
[184] Ibid.
[185] Business Tech 'Crime Data shows South Africa's murder rate on the rise' available at: https://businesstech.co.za/news/lifestyle/539532/crime-data-shows-south-africas-murder-rate-on-the-rise/ accessed on 18 January 2022.
[186] Nicole McCain News24 'Police ordered to pay R140m for misconduct over five months' available at: https://www.news24.com/news24/southafrica/news/police-ordered-to-pay-r140m-for-misconduct-over-five-months-report-20210621 accessed on 18 January 2022.
[187] Ibid.
[188] Nic Andersen 'Cops are losing the war on crime' available at: https://www.thesouthafrican.com/news/cops-are-losing-the-war-on-crime-police-officials-alarming-revelation-on-crime/ accessed on 18 January 2022.
[189] Ibid.
[190] Supra note 97 at s55.
[191] Ibid.

digital or computer forensics was needed to aid detectives in the discovery and subsequent detection of cybercrime.[192] This resulted in the establishment of cyber inspectors, as mandated by the ECT Act, which was passed more over a decade ago.[193]

However, South Africa today has a scarcity of experienced and competent forensic professionals.[194] According to forensic expert Jason Jordaan's 2017 submission on the Cybercrimes Bill to the South African Portfolio Committee on Justice and Correctional Services, based on research on the quality assurance of digital forensics in South Africa currently, only 59% of forensic practitioners have completed an undergraduate degree or diploma, with only 43% having an undergraduate qualification relevant to the practice of digital/ computer forensics[195]. Only 0.09% of practitioners with a Bachelor of Science degree in Computer Science, one of the particular certifications required for digital forensics, hold a Bachelor of Science degree.[196] Finally, just 23% of digital/computer practitioners have a postgraduate degree.[197]

To provide for a competent and qualified operational capability to identify and investigate cybercrime, the aforementioned problems must be completely addressed. "The cybercrimes Act is not a silver bullet; we still lack the capabilities to apprehend cyber criminals", says the director of the Electronic Crime Unit of South Africa's investigative authority, the Hawks.[198]

4.4 Major obligation placed on ECSP's:

The anonymity of the internet appeals to the majority of cybercriminals.[199] The global information system is free, and there is no information about who a user is or where they are at any given time.[200] This makes it more difficult to determine a user's identity, especially if

[192] Sutherland A 'Governance of cybersecurity – The case of South Africa' 2017 *AJLC* 83 2077-7213.
[193] Ibid.
[194] Sutherland op cit note 192.
[195] Jordaan, J 'Submissions on the Cybercrimes and Cybersecurity Bill' available at pmg.org.za/files/170913DFIRLABS.pdf (10 August 2017) Accessed on the 20 August 2022.
[196] Ibid.
[197] Jordaan op cit note 195.
[198] Brigadier Piet Pieterse, Head of the Electronic Crime Unit of the Hawks, made this statement in 2015. See S Naik & R Serumula 'Dark Web thriving in SA' (17 October 2015) available at: https://www.iol.co.za/news.south-africa/dark-web-thriving-in-sa-1931641. Accessed on the 20 august 2022.
[199] Sommer 'Against Cyberlaw' (2000) *Berkley Technology LJ* 1154-1232 at 1168.
[200] Ibid.

the person hides their location by using several search engines at different times.[201] Cybercriminals can mask their identities since there is unrestricted freedom in cyberspace.[202]

When a cybercrime is reported, for example, by an ECSP in accordance with their duties under Section 54 of the Act, the Act requires ECSPs to provide details to the court.[203] The court may request, *inter alia*, the electronic communications identity number from which the data message originated and whatever information that an electronic communications service provider has access to that might help the court identify the person.[204]

There is significant concern about this provision, particularly the details on the person's identity number, surname, and address. The provision fails to account for instances where the electronic communication is stolen, or the identity number is falsified by a perpetrator using someone else's identity.

An example of the above scenario can be seen in the case of Sony Pictures[205] whose security was attacked by a series of spear phishing emails addressed to Sony employees.[206] After researching employee names and positions on LinkedIn, hackers posed as colleagues, sending phishing emails with malware to unsuspecting employees.[207] In the end, more than 100 gigabytes of corporate data were taken, including freshly released files, financial records, and client information.[208] Sony lost more than $100 million as a result of the phishing attack.[209]

Cybercriminals are able to commit crimes by using false information that cannot be traced back to them. Even if the cybercrime is prosecuted, it is unlikely to result in a successful outcome because the information used by the hackers is fake. The Cybercrimes Act, which mandates

[201] Sommer op cit note 199 at 1168.
[202] Ibid.
[203] Supra note 97 at s21(1)(b).
[204] Ibid.
[205] Aaron Mamiit, Tech Times 'Sony Pictures Cyber Attack may cost $100million, says experts' available at: https://www.techtimes.com/articles/21869/20141210/sony-pictures-cyber-attack-may-cost-100-million-says-expert.htm accessed on 18 January 2022.
[206] Gregg Keizer 'Sony hackers targeted employees with fake Apple ID emails' (2015) available at: https://www.computerworld.com/article/2913805/sony-hackers-targeted-employees-with-fake-apple-id-emails.html accessed on 13 August 2021.
[207] Ibid.
[208] Gregg op cit note 190.
[209] Ibid.

companies to provide information about their communications with hackers, is insufficient because the hackers use personal information from actual employees, making it difficult to identify the actual perpetrators. Requiring ECSPs to provide information is not a practical or adequate solution to identifying cybercriminals.

4.5 Prosecution of cyberthreats in South Africa:

As described in the preceding chapter, the Serious Commercial Crimes Unit (SCCU) prosecutes serious, complicated, and organized commercial crime in the SCCCs, which are dedicated courts on the regional court tier.[210] SCCCs are Regional Magistrates Courts, the only courts in the country that are not governed by legislation. The Constitutional Court, Magistrates Courts, Equality Court, Labour Court, and Labour Appeal Court, for example, are all courts in the country that are formed or constituted in accordance with some piece of legislation or regulation.[211] However, the SCCC is not particularly named as the go-to court for prosecuting cyber risks.[212]

The Act, in section 24, incorporates a jurisdictional aspect, as discussed in the preceding chapter; nonetheless, the issue of the SCCC's activities as the forum for the prosecution of cyber threats would continue without enabling legislation, risking the proceedings being deemed illegal. The principle of legality (*nullum crimen sine lege*), enshrined in section 35(3)(l) and (n) of the Constitution, is central to the rule of law and respect of human dignity.[213] It demands that the state not exercise power over anyone unless it does so within the law.[214]

The selection of which form of cybercrime will be prosecuted at the SCCCs is one example of the consequences of the absence of regulation in this respect.[215] This was recently highlighted in the NDPP's perplexing report, which said that cybercrime was prosecuted by the Serious Business Crimes Unit without separating the commercial aspect that should be punished exclusively at the SCCCs.[216]

---

[210] Altbeker A Monograph 76: Justice through specialization? The case of the specialized commercial crimes court. (Pretoria: Institute of Security Studies 2003).
[211] Ibid.
[212] Altbeker A op cit note 210.
[213] *Constitution of the Republic of South Africa 1996.*
[214] Ibid.
[215] Altbeker A op cit note 210.
[216] Ibid.

Furthermore, the absence of legislation extending the SCCCs' jurisdiction can be deduced from the need for the SAPS investigator connected with the SCCC to approach the High Court for an order to intercept indirect or real-time communications as part of his or her detection of the crime, which is generally accepted to have cross-border dimensions.[217]

The nature of cyber threats as a cross-border crime and related issues were on display in the Western Cape Division of the High Court, when a final sequestration order was confirmed against a foreign citizen located in Cape Town who cheated a victim in the United States.[218] A total of $15 million USD was deposited into the perpetrator's South African bank account. He then transferred a major chunk of the money to several bank accounts abroad, leaving the victim with irreversible losses.[219] Section 21 (2) of the SCCU determined jurisdiction in this case based on the respondent's residency. It is true that when cybercrime is found, crime detectives must be able to act promptly or the electronic trail would become cold. This danger is increased by the necessity to appeal the order to the High Court.[220]

[217] Altbeker A op cit note 210.
[218] Ibid.
[219] Altbeker A op cit note 210.
[220] Ibid.

CHAPTER 5: RECOMMENDATIONS

5.1 To address the shortcomings of investigative units put in place:

The provisions of the Cybercrimes Act can effectively be used to investigate and successfully prosecute cybercrimes facilitated by cyber threats toward companies. However, there seems to be a disconnect between the provisions of the Act and the status quo of South Africa.

With regards to the Designated Point of Contact clause, the SAPS is in charge of overseeing investigations under the Act, but there are severe shortage of skills, expertise, and people.[221] Karen Allen advises that South Africa seek foreign financiers as well as interact with Interpol and business sectors to gather resources, mentorship, and knowledge transfer in order to bridge this capacity gap.[222]

The project's goal is to promote intelligence-led, coordinated operations against cybercrime and its perpetrators in African member countries by creating a standardized regional coordination framework for drafting joint action plans and executing law enforcement

[221] Karen Allen 'South Africa Lays Down the Law on Cybercrime' (2021) available at: https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime Accessed 13 August 2021.
[222] Ibid.

actions.[223] The Africa Cybercrime Operation Desk, housed in INTERPOL's Cybercrime Directorate, would be central to the initiative.[224] The desk will create and implement the framework, as well as conduct joint operations, enhancing Africa's ability and capabilities to combat cybercrime.[225]

Activities will focus on both prosecuting cybercrime criminals in Africa and preventing it.[226] While the preventive programs will seek wide regional participation, the operational actions will concentrate on nations who have already actively engaged with our Cybercrime Directorate to build a baseline for these operations.[227]

South Africa would benefit from working with a larger entity with resources and influence by engaging with groups such as INTERPOL.[228] A dedicated agency like this one has devoted manpower to combat cybercrime as well as shared understanding with other countries.[229] It brings together international and regional law enforcement authorities through the INTERPOL conversation to guarantee a coordinated response to global security concerns.[230]

5.2 To address the attainment of requisite skills:

With regards to section 55 of the Act which places an obligation on the South African government to ensure that there is an establishment of an operational capacity to detect and investigate cybercrimes.[231] It is unfortunate that the Act fails to realise that these skill sets are scarce in the country, as illustrated in the previous chapter.

Academic author, Cross, explains that it should be apparent that cybercrime detectives need broad training to work efficiently in this specialty area.[232] This need is usually acknowledged

[223]INTERPOL: 'African joint operation against cybercrime' available at: https://www.interpol.int/en/crimes/cybercrime/cybercrime-operations/afjoc-african-joint-operation-against-cybercrime accessed on 2 October 2021.
[224] Ibid.
[225] INTERPOL op cit note 223.
[226] Ibid.
[227] INTERPOL op cit note 223.
[228] Ibid.
[229] INTERPOL op cit note 223.
[230] Ibid.
[231] Supra note 97 at s55.
[232] Cross 'Scene of the cybercrime' 2nd ed (2008) *Burlington: Syngress publishing Inc.*

in wide law enforcement agencies, where IT professionals and computer sciences might be enrolled to handle cybercrime investigations. [233]

Examples of categories of cyber investigators by skill set involve the following:[234]

A) The detectives who specialized in computer/ network crime. They are detectives first with a secondary interest.[235]
B) Computer experts who conduct investigations. They are information Technology Professionals first, with a secondary interest in law enforcement and in investigation.[236]
C) Those who qualify skilled, skilled or interested in investigation and IT. they are involved in computers/cybercrime from the beginning of their careers, they have equivalent training in both fields, such as a double main in criminal justice and network engineering programming.[237]
D) Those who have not skilled or attracted in either investigation or IT. These could be police officials who were sent to the investigation division and drew a cybercrime case casually. They aren't really attracted in the investigative field and would desire to be working patrol.[238]

The author believes that the Cybercrimes Act can be more effective in investigating and prosecuting cybercrimes with proper training and resources. Adequate training for government officials and police in computer-related skills can improve their understanding of the Act and lead to more effective methods. Extensive training for police is necessary to combat cybercrimes and other online crimes.

5.3 Major obligations placed on ESCPs:

[233] Ibid.
[234] Cross op cit note 232.
[235] Ibid.
[236] Cross op cit note 232.
[237] Ibid.
[238] Cross op cit note 232.

As noted in the preceding chapter, when an ESCP reports a crime, businesses are required by section 54 of the Cybercrimes Act to provide any information that they have.[239] It was also demonstrated in the previous chapter that this information might be fraudulent, and if a cybercriminal cannot be identified, a company might experience difficulty in successfully claiming monetary damages.

Companies can remedy the deficiency in the Cybercrimes Act by investing in cybersecurity infrastructure. Companies can recruit cybersecurity-savvy programmers. Programmers have devised deft methods for obtaining information about hackers following a cybercrime.[240] Many programmers, for example, utilize Python Traceback. This coded language, also known as Back-tracing (or traceback), is the process of tracking down the offender or digital equipment used to commit a cybercrime.[241] A preliminary inquiry is carried out to expose information about the cybercrime by an analysis of log files, for instance, through event logs which are files produced by systems as a result of activity.[242] This method can provide information about the cybercrime and how it occurred.[243]

For example, event logs "automatically record... events that occur within a computer to provide an audit trail that may be used to monitor, understand, and diagnose network activities and problems".[244] "These logs include application logs, which record "events logged by programs and applications", and security logs, which "document all login attempts (both legitimate and erroneous) and the installation, opening, or deletion of files, programs, or other objects by a computer user".[245] These event logs may provide information on the IP address utilized in the cybercrime.[246]

[239] Supra note 97.
[240] Edward Krueger & Douglas Franklin 'A simple way to trace code in Python' available at: https://towardsdatascience.com/a-simple-way-to-trace-code-in-pythod-a15a25cbbf51 accessed on 1 October 2021.
[241] Ibid.
[242] Edward op cit note 240.
[243] Ibid.
[244] Miller, L 'Cyber Insurance: An incentive alignment solution to corporate Cyber-insecurity' 7(2) (2019) *Journal of Law & Cyber Warfare* 147-182 at 150.
[245] Ibid.
[246] Edward op cit note 240.

This is only one of many examples of how businesses may help solve problems. This avoids providing inaccurate information to investigators and contributes meaningfully to the inquiry. Many academic authors believe that IT experts and government authorities should work together to tackle the rising cyberattacks. This objective can still be attained by companies and IT specialists working together to locate reliable facts to contribute to a State-led probe.

5.4 Establishment of statutory SCCCs.

The final recommendation is in regard to the forum where cybercrimes is to be prosecuted in South Africa. This author recommends that existing courts legislation and regulations governing magistrates' courts be amended, or new legislation and regulations be developed, to establish the SCCCs or similar courts as the preferred for a for the prosecution of commercial cybercrime, including cyber threats in the country upon the finalization of laws combating cybercrime.[247] The SCCCs are the only courts in the country not founded in legislation or regulation.[248] It is therefore submitted that in legislating the establishment of the SCCCs, this anomaly will be corrected.[249] Additionally, it will solve the problem of a timely prosecution and resources involved in the activities of the investigators.[250] This may be resolved according to the SCCCs jurisdiction akin to that of the High Court as has been done with the case of Divorce Courts, which, like the SCCCs, are located in the Magistrates Courts.[251]

[247] Sukardi, D 'Legal protection against cyber-crime threats for business economics' 11(4) (2022) *Legal brief* 2227-2235 at 2228 – 2230.
[248] Ibid.
[249] Altbeker op cit note 210.
[250] Ibid.
[251] Altbeker op cit note 210.

CHAPTER 6: CONCLUSION:

This report sought to evaluate first, whether South Africa's legislation governing the detection and prosecution of cybercrime threats are effective and secondly, whether companies can rely on South African law enforcement for adequate protection against cybercrime threats.

In concluding the first aspect, the author has come to the conclusion that the current legislation of governing cybercrime threats in South Africa is effective. Chapter 2 of the Act adequately criminalizes cybercrime threats and the Act goes a step further to make provision in the instance where these cybercrime threats do not materialize, the Act categorizes this instance as cyber extortion under section 10 and it is effectively criminalized. The author is of the opinion that on the face of it, a detailed analysis of the Act seems to adequately and effectively offer investigative methods and prosecution methods. However, one cannot be certain due to the Act being so new, there is not much to compare the practicality of the Act to. This author investigated the Acts provisions against the status quo of South Africa and found that a major focus needs to be placed on the attainment of requisite skills. All investigative- role players need to be adequately trained and molded for the role that is being bestowed upon them by the

Act. This will ensure a more effective way in which cybercrime in South Africa will be combatted.

In concluding the second aspect, the author is of the opinion that while there are measures in place to which companies can turn, because of the disconnect from the provisions of the Act and the status quo of South Africa, this author recommends that companies could mitigate the pressure of law enforcement by taking proactive steps in helping law enforcement combat crime. The Act places an onerous obligation on ECSPs and the Act sort of tucks companies into the category of an "investigative role player". One of the ways in which companies can ensure their existence is not threatened is to is to obtain cybersecurity insurance.[252] Cybersecurity insurance is designed to safeguard against losses caused by a variety of cyber disasters, such as data breaches, business interruption, and network damage.[253] A thriving cybersecurity insurance market might assist minimize the frequency of successful cyber-attacks by first promoting the use of preventative measures in return for increased coverage;[254] second, by basing premiums on an insured's level of self-protection, premiums are encouraged to be implemented best practices.[255]

Traditional commercial general liability and property insurance policies frequently exclude cyber risks, necessitating the emergence of cybersecurity insurance as a "stand alone" line of coverage.[256] This coverage shields companies against a wide range of cyber event losses that they may directly or indirectly cause to others.[257]

Since 2012, CISA has collaborated with academia, infrastructure owners and operators, insurers, chief information security officers (CISOs), risk managers, and others to create strategies to improve the cybersecurity insurance market's capacity to address this growing cyber risk sector.[258] CISA has also sought comments from these same stakeholders on the market's ability to compel enterprises to improve their cybersecurity in return for more

[252] Cybersecurity & Infrastructure security agency available at: http://www.cisa.gov/cybersecurity-insurance accessed on 4 October 2021.
[253] Ibid.
[254] Sukardi op cit note 247 at 2230.
[255] Ibid.
[256] Cybersecurity op cit note 252.
[257] Ibid.
[258] Cybersecurity op cit note 252.

coverage at a cheaper cost.[259] CISA is actively fostering discussions with CISOs, Chief Security Officers (CSOs), and insurers about how a cyber threat data repository could aid in the discovery of emerging cybersecurity methodologies across industries, as well as the emergence of new cybersecurity insurance policies that "benefit" businesses for implementing such best practices.[260]

BIBLIOGRAPHY

Books

1. Brian, C 'Cyberlaw: The Law of the Internet and Information Technology' (2020) *Pearson Education* 1-288.
2. Brownsword, R., Goodwin, M., & Johnston, A 'Law and the Technologies of the Twenty-First Century: Text and Materials' (2012) *Cambridge University Press* 453.
3. Burchell J 'Criminal Justice at the Crossroads' (2002) 19 *SALJ* 585.
4. Cross, M 'Scene of the cybercrime' 2nd ed (2008) *Burlington: Syngress publishing Inc* 725.
5. Holt, T. J., & Bossler, A.M 'Cybercrime and Digital Forensics: An introduction' (2015) *Routledge* 1-812.
6. Papadopoulos, S & Snail, S 'Cyberlaw @ SA III: The law of the internet in South Africa' (2012) 3 *Van Schaik*.

[259] Ibid.
[260] Cybersecurity op cit note 252.

7. Papadopoulos, S & Snail, S 'Cyberlaw @ SA The Law of the Internet in South Africa 4/e' 4th ed (2022) *Van Schaik Publishers.*
8. Sarfraz, M 'Cybersecurity Threats with New Perspectives' ed (2021) *intechopen* 178.
9. Theophilopulos, C., van Heerden, CM., Boraine, A 'Fundamental Principles of Civil Procedure' (2015) third edition 1-495.
10. Van der Merwe 'Information and Communications Technology Law' 3rd ed (2021) *LexisNexis* 795.
11. Wasik, M 'Crime and the Computer' (1991) *Oxford: Clarendon Press* 159-160.
12. Watney, M 'Cybercrime and the investigation of cybercrime" in Papadopoulos S and Snail S (eds) *Cyberlaw@ SA III The Lay of the internet in South Africa* 3rd ed 333-350 (Van Schaik 2012).

Chapters in Books

1. Cassim, F 'Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players' 44 (1) (2011) *The Comparative and International Law Journal of Southern Africa* 123-138 at 129-134.
2. Sommer 'Against Cyberlaw' (2000) *Berkley Technology LJ* 1154-1232 at 1168.

Journal Articles

1. Aggarwal, P, et al. 'Random Decision Forest approach for Mitigating SQL Injection Attacks' (2021) *International Conference on Electronics, Computing and Communication* 1-5.
2. Alenezi, M. N, Alabdulrazzaq H, Alshaher A & Alkharang M.M 'Evolution of malware threats and techniques: A review' 12 (3) (2020) *International Journal of communication networks and information security* 326-337.
3. Altbeker ,A "A model for justice delivery: The Specialised Commercial Crime Court" (2016) *Research gate* 31-34.

4. Altbeker, A Monograph 76: Justice through specialization? The case of the specialized commercial crimes court. (Pretoria: Institute of Security Studies 2003).
5. Arkin, et al 'Prevention and Prosecution of Computer and high technology crime' (1990) 1-1.
6. Basdeo, V 'The Constitutional Validity of Search and Seizure Powers in South African Criminal Procedure' 19 (2009) *PER/PELJ* 307-360.
7. Brenner, S W 'Prosecuting Cybercrime: Challenges and Solutions' 97 (2007) *Journal of Criminal Law and Criminology* 1361-1395.
8. Cashell, B, et al. 'The Economic impact of cyber-attacks' 2 (2004) 2 *Congressional research service documents, CRS RL32331 (Washington DC)* 1-41.
9. Cassim, F 'Formulating Specialized Legislation to Address the Growing Specter of Cybercrime: A Comparative Study' (2009) 12(4) *PER* 360.
10. Chauhan, A 'Evolution and Development of Cyberlaw – A Study with Special reference to India' (2013) *SSRN* 1-18.
11. Chen, C D 'Computer crime and the Computer Fraud and Abuse Act of 1986' (1990) 10(1) *Computer Law Journal* 71-86.
12. Dhamija, R, Tygar, D and Hearst, M 'Why phishing works' (2006) *Proceedings of the SIGCHI conference on Human Factors in computing systems* 581-590.
13. Dumchikov, M, Fomenko, A, Yunin, O, Pakhomov, V & Kabenok, Y 'The essence and classification of cybercrime in the field of computer information' 11(51) (2022) *Revista Amazonia Investiga* 291-299.
14. Ezeji, C. L., Olurola, A. A., & Bello, P. O. 'Cyber-related crime in South Africa: extent and perspective of state's roleplayers' 31(3) (2018) *African Journal of Criminology & Victimology'* 93-110.
15. Gerstein, D.M 'Better Anticipating and Managing Today's Growing Cyber Risks' 7 (4) (2022) *The Cyber Defense Review* 15-30.
16. Gokhale, G 'Network analysis of dark web traffic through the geo location of South African IP address' (2020) *Smart cities performability cognition and security* 201-219.
17. Gordon, F., McGovern, A., Thompson, C., and Wood, M. A 'Beyond cybercrime: New Perspectives on crime, and digital technologies' 11(1) (2022) *International Journal for Crime, Justice and Social Democracy. Brisbane, Queensland, Australia: Queensland University of Technology* 1-8.

18. Halfond, W, Viegas, J and Orso, A 'A classification of SQL-injection attacks and countermeasures' (2006) 1 *In proceedings of the IEEE international symposium on secure software engineering* 13-15.
19. Kader, S and Minnar, A 'Cybercrime investigations: Cyber-process for detecting of cybercriminal activities, cyber-intelligence and evidence gathering' 5 (2015) *Acta Criminologica: SAJC* 124- 134.
20. Khan, S, Saleh, T, Dorasamy, M, Khan, N, Leng, O & Vergara, R 'A systematic literature review on cybercrime legislation' 11 (2022) *F1000 Research* 971.
21. Lakshmi, P.V.S 'SQL Injection detection analysis using deep learning' 8 (2022) *Journal of Engineering Sciences* 13 at.
22. Lessig, L 'The Law of the horse: What cyberlaw might teach' (1999) 113 *Harvard Law Review* 501-549.
23. Mabunda , S 'Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill' (2018) *Statute Law Review* 9. doi:10.1093/slr/hmx028.
24. Manhas, S 'An Interpretive Saga of SQL Injection Attacks- Emerging Technologies in Data mining and information security' 1 (2022) *Proceedings of IEMIS, Singapore: Springer Nature Singapore* 1-3.
25. Markus, J 'The rising threat of launchpad attacks' (2019) 17(5) *IEEE Security & Privacy* 68-72.
26. Miller, L 'Cyber Insurance: An incentive alignment solution to corporate Cyber-insecurity' 7(2) (2019) *Journal of Law & Cyber Warfare* 147-182.
27. Organization for Economic Co-operation and Development, 2004.
28. Plachta, M & Zagaris, B 'Economic Sanctions' 38 (2022) *IELR* 291.
29. Ramluckan, T 'International Humanitarian Law and its Applicability to the South African Cyber Environment' 19(3) (2020) *Journal of Information Warfare* 102-117.
30. Robert, L and Hamrock, J 'Using entropy analysis to find encrypted and packed malware' (2007) 5(2) *IEEE Security & Privacy* 40-45.
31. Rudner, M 'Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge' (2013) 26 *International Journal of Intelligence and Counterintelligence* 453- 481.
32. Salter, M, R. and Van Erp, J, M 'Prosecuting Cybercrime: An international Perspective' 1 (2021) *International Journal of Cybersecurity Intelligence and Cybercrime* 47- 61.
33. Sieber, U 'New Legislative Responses to Computer-related economic crisis' 76 (1986) *The International Emergence of Criminal Information Law* 5.

34. Singh, N & Tiwari, P 'SQL Injection Attacks, Detection Techniques on Web Application Databases. In Rising Threats in Expert Applications and Solutions: Proceedings of FICR-TEAS. (2022) *Singapore: Springer Nature Singapore* 387-394.
35. Sukardi, D 'Legal protection against cyber-crime threats for business economics' 11(4) (2022) *Legal brief* 2227-2235.
36. Sutherland A 'Governance of cybersecurity – The case of South Africa' 2017 *AJLC* 83 2077-7213.
37. Ulrich, B, et al. 'Scalable, behavior-based malware clustering' (2009) 9 *NDSS* 8-11.
38. Van Vuuren, J. J., Leenen, L,. & Pieterse, P 'Development and Implementation of Cybercrime Strategies in Africa with Specific Reference to South Africa' 19(3) (2020) *Journal of Information Warfare* 83-101.
39. Watney, M, M 'Die strfregtelike en prosedurele middele ter bekamping van kubermisdaad' (deel 1) (2003) *TSAR* 56.

Legislation

1. *Constitution of the Republic of South Africa 1996.*
2. *Criminal Procedure Act 51 of 1977 of South Africa.*
3. *Cybercrimes Act 19 of 2020 of the Republic of South Africa.*
4. *Protection of Personal Information Act 4 of 2013 of South Africa.*
5. *The Electronic Communications and Transactions Act 25 of 2002 of South Africa.*
6. *The Promotion of Access to Information Act 2 of 2000 of South Africa.*
7. *The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 of South Africa.*

Internet sources

1. Aaron Mamiit, Tech Times 'Sony Pictures Cyber Attack may cost $100million, says experts' available at: https://www.techtimes.com/articles/21869/20141210/sony-pictures-cyber-attack-may-cost-100-million-says-expert.htm accessed on 18 January 2022.
2. Brigadier Piet Pieterse, Head of the Electronic Crime Unit of the Hawks, made this statement in 2015. See S Naik & R Serumula 'Dark Web thriving in SA' (17 October

2015) available at: https://www.iol.co.za/news.south-africa/dark-web-thriving-in-sa-1931641. Accessed on the 20 august 2022.

3. Business Tech 'Crime Data shows South Africa's murder rate on the rise' available at: https://businesstech.co.za/news/lifestyle/539532/crime-data-shows-south-africas-murder-rate-on-the-rise/ accessed on 18 January 2022.
4. Cybersecurity & Infrastructure security agency available at: http://www.cisa.gov/cybersecurity-insurance accessed on 4 October 2021.
5. Edward Krueger & Douglas Franklin 'A simple way to trace code in Python' available at: https://towardsdatascience.com/a-simple-way-to-trace-code-in-pythod-a15a25cbbf51 accessed on 1 October 2021.
6. Gregg Keizer 'Sony hackers targeted employees with fake Apple ID emails' (2015) available at: https://www.computerworld.com/article/2913805/sony-hackers-targeted-employees-with-fake-apple-id-emails.html accessed on 13 August 2021.
7. https://www.saps.gov.za/dpci/reportingguide.php
8. INTERPOL: 'African joint operation against cybercrime' available at: https://www.interpol.int/en/crimes/cybercrime/cybercrime-operations/afjoc-african-joint-operation-against-cybercrime accessed on 2 October 2021.
9. Jordaan, J 'Submissions on the Cybercrimes and Cybersecurity Bill' available at https://www.pmg.org.za/files/170913DFIRLABS.pdf (10 August 2017) Accessed on the 20 August 2022.
10. Johan Burger and Stuart Mbanyele 'Old Solutions won't fix South Africa's deteriorating police service' available at: https://issafrica.org/iss-today/old-solutions-wont-fix-south-africas-deteriorating-police-service accessed on 18 January 2022.
11. Karen Allen 'South Africa Lays Down the Law on Cybercrime' (2021) available at: https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime Accessed 13 August 2021.
12. Nic Andersen 'Cops are losing the war on crime' available at: https://www.thesouthafrican.com/news/cops-are-losing-the-war-on-crime-police-officials-alarming-revelation-on-crime/ accessed on 18 January 2022.
13. Nicole McCain News24 'Police ordered to pay R140m for misconduct over five months' available at: https://www.news24.com/news24/southafrica/news/police-ordered-to-pay-r140m-for-misconduct-over-five-months-report-20210621 accessed on 18 January 2022.