THE SOUTH AFRICAN LEGISLATIVE RESPONSE TO CYBERCRIME

Thesis submitted in fulfilment of the requirements for the PhD

in the

Department of Criminal Justice and Procedure

Faculty of Law

UNIVERSITY OF THE WESTERN CAPE

SAGWADI MMAHLATSE MABUNDA

3568998

Supervisor: Prof RA Koen

Co-Supervisor: Prof AJ Hamman

2021

Declaration

I, Sagwadi Mmahlatse Mabunda, declare that **The South African Legislative Response to Cybercrime** is my own work, that it has not been submitted before for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged as complete references.

Student: SAGWADI MABUNDA

Signed:

Date: 3 November 2021

Supervisor: PROFESSOR RA KOEN (Retired)

Co-Supervisor: PROFESSOR AJ HAMMAN

Signed:

Date: 3 November 2021

Dedication

This paper is dedicated to my parents, Calvin and Sarah Mabunda. Papa, *ni khensa ku kombiwa ndlela.* Mama, *ni khensa swikhongelo swa n'wina*. To the Almighty God, *Xikwembu xa tintswalo, Hosi ya mina, U kahle*.

"The LORD will fulfil His purpose in me. O LORD, Your loving devotion endures forever--do not abandon the works of Your hands."

—Psalm 138:8

Acknowledgments

I am very grateful to my supervisor Professor Raymond Koen of the Faculty of Law University at the Western Cape for your dedicated supervision and support. Thank you for challenging me and believing in me even when I did not believe in myself.

Prof Lovell Fernandez, Prof Jamil Mujuzi and Prof Abraham Hamman, thank you for betting on me. To my friends in the Department of Criminal Justice and Procedure, thank you all for taking this journey with me.

I am grateful for the South African National Research Foundation's generous support throughout this project.

To my Cape Town friends and family, you have made it worthwhile. Thank you to my friends at Every Nation Church for taking care of me and believing in me. Special thanks to the Africas, the Tities', the Prins' and the Jacobs' for adopting me and making me one of your own. My dear friends Dr Sibanda, Mr Maphosa and Mr Edison, thank you for the support and mentorship. Sivuyisile Mcilongo, we did it, kiddo!

To my family, thank you for your unwavering support, thank you for understanding my long absences. A special thanks to my sisters Rhulani Thobakgale and Tinyiko Mabunda and to my brother Mashudu Thobakgale for cheering me on. My love to my wonderful babies, my nieces and nephews, Lutendo, Ofuna, Onea, Ntshovelo, Ntshembo and Ntsumi, this is for you. Finally, to my dear brother Dzunani Mabunda, I miss you and thank you for watching over me, I hope I have made you proud.

And finally, Mbulelo Fingers, you are God's love personified.

Table of Contents

Abstract

As the world moves into a hyper-connected global society with near universal access to the internet, cybercrime has become a global challenge.

The problems embedded in the issue of cybercrime are at least twofold. Firstly, the proliferation of cybercrime globally, and more specifically in South Africa, is outstripping the pace at which governments and lawmakers are able to respond efficiently. Secondly, where governments do manage to respond, there is a temptation to do so on the basis of a superficial understanding of the essence of cybercrime.

There are many debates about the novelty of cybercrime in which participants have described it as “old wine in new skin”. This study takes the position that cybercrime is neither completely novel nor is it merely a virtual manifestation of the ordinary terrestrial crimes. The premise of this research is that cybercrime is an interesting and unique form of criminality that manifests itself in a number of challenging ways. These manifestations need to be considered independently and comprehensively if effective countermeasures are to be devised. This is not to say that every single offence has to be considered critically. That would be impracticable. It would suffice that certain types of cybercrimes be classified differently from other types, so as not to paint all with the same brush.

This study therefore wants to determine whether there are certain parameters that can be set which will determine what constitutes cybercrime? In other words, given the complexity of cybercrime, is it possible to outline a threshold for which kinds of acts would qualify as true cybercrimes and which would not, in order to determine the acts for which the South African Cybercrimes Act ought to have made provision?

This study seeks to answer this question. It adopts a two-part framework based on the Gordon & Ford Classification of Cybercrime and the Routine Activities Theory.

Key Words

Artificial Intelligence

Availability

Capable Guardian

Confidentiality

Cyber-Capable Guardian

Cybercrime

Designated Point of Contact

Gordon & Ford Classification

Integrity

Legislation

Machine Learning

Motivated Offender

Routine Activities Theory

Suitable Target

True Cybercrimes

Type I Cybercrimes

Type II Cybercrimes

Abbreviations and Acronyms

AI	Artificial Intelligence
CDA	Communication Decency Act
CIA Triad	Confidentiality, Integrity and Availability Triad
CoE	Council of Europe
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPoC	Designated Point of Contact
ECTA	Electronic Communication and Transactions Act
FBI	Federal Bureau of Investigation
FICA	Financial Intelligence Centre Act
G&FC	Gordon & Ford Categorisation
ICCMA	International Co-operation in Criminal Matters Act
ICT	Information and Communications Technology
ISP	Internet Service Provider
ITU	International Telecommunication Union
ML	Machine Learning
NCSC	National Cyber Security Centre
NDPP	National Director of Public Prosecutions
NIST	National Institute of Standards and Technology
NPA	National Prosecuting Authority
POCA	Prevention of Organised Crime Act
RAT	Routine Activities Theory
SALRC	South African Law Reform Commission
SAPS	South African Police Services
SITA	State Information and Technology Agency
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
VoIP	Voice of Internet Protocol

CHAPTER ONE

LANDSCAPE OF CYBERCRIME

1.1 Introduction: The Challenge of Cybercrime

By 2011, at least 2.3 billion people globally had access to the internet, a figure which is equivalent to one third of the world's population. More than 60 per cent of all internet users lived in developed countries and about 45 percent of them were below the age of 25 years. It was estimated that by the year 2017, subscriptions to mobile broadband would have encompassed more than 70 per cent of the world's population.[1] As of June 2020, it was estimated that there are over 4.13 billion internet users with China being the country with the biggest number of internet users.[2]

Information and Communication Technologies (ICTs) have become indispensable in modern society. As a result of the interconnectivity of computer networks, ICTs play a critical role in economic growth, education and citizen participation in social media.[3] As the world moves into a hyper-connected global society with near universal access to the internet,[4] it is hard to imagine any "computer crime" that will not involve internet connectivity and interaction with cyberspace. These technological advancements require fundamental changes in the approaches to law enforcement, investigations and evidence gathering, and issues surrounding international co-operation.[5] The dangers posed by cybersecurity threats are real and they have created a concomitant need for the development of adequate security measures.[6]

There have been numerous cyber-attacks against advanced information societies which have had the goal of undermining and disrupting the functioning of public and private

1 UNODC Study (2013) at xvii. According to the International Telecommunications Union (ITU) internet users are defined as "…individuals who have used the Internet (from any location) in the last 3 months. The Internet can be used via a computer, mobile phone, personal digital assistant, games machine, digital TV etc."

2 Clement (2020) at 1. ITU World Telecommunication/ICT Indicators Database at 1.

3 National Cybersecurity Policy Framework (2015) at 70. Roztocki, Soja & Weistroffer (2019). Johannes König, Daniela J. Jäger-Biela & Nina Glutsch (2020) at 610.

4 Schneier (2018) at 5.

5 Grobler (2012) at 1.

6 National Cybersecurity Policy Framework (2015) at 70.

sector information systems. These have placed the security of cyberspace and ICTs on the high priority agendas at national and international levels. No one is immune to cybercrime, as the South African Department of Justice and Transnet discovered when they both experienced ransomware attacks within months of each other in the second half of 2021.[7]

Africa was the last continent to embrace ICTs, and a decade ago only a handful of African countries had local internet access.[8] There has been since a monumental growth in the adoption of ICTs across sub-Saharan Africa.[9] However, this occurred in the context of inadequate telecommunications infrastructure. What is more, there have been serious impediments to securing uninterrupted access to innovative information technology advances such as e-governments, e-commerce and telemedicine.[10] Sub-Saharan Africa, whilst showing growth, is home to 47% of the world's uncovered population when it comes to mobile internet connectivity – this amounts to about 210 million people as of 2019. Be that as it may, the region has seen increased growth in coverage with the roll out of 3G and 4G in West and East Africa with more than a quarter (28%) of the population in the region using mobile internet. This is more than double the usage level in 2014.[11]

The endless possibilities created by internet connectivity for billions across the world have created also unlimited capabilities for those tied to the criminal world. Those who wish to engage in criminal activities have taken full advantage of the internet's power to commit a host of cybercrimes.[12] As noted above, in recent years Africa has witnessed explosive growth in ICTs. However, expanding bandwidth and increases in the use of wireless technologies and infrastructure have been coupled with high levels of computer illiteracy and insufficient or ineffective regulatory measures, making African countries especially vulnerable to cybersecurity breaches.[13]

The phenomenal growth of internet connectivity in Africa is due largely to the extensive investment in ICT infrastructure, particularly from the developed world. Just as

7 Department of Justice and Constitutional Development (2021) at 1; Ngqakamba (2021) at 1; Toyana (2021a) at 1 and Toyana (2021b) at 1.
8 Longe (2009) at 155.
9 Asongu & Biekpe (2017) at 4.
10 Longe (2009) at 156
11 Delaporte (2021) at 14.
12 Stander (2009) at 217.
13 Grobler (2012) at 1; Gumbi (2018) at 11.

with other investment opportunities, Africa has lucrative potential for international investors in ICT infrastructure.[14] Unfortunately, it would appear that these investments are not supported by regular upgrades and updates, leaving them vulnerable to cybercriminality.[15] Many African states, including South Africa, claim to have the best and most expensive security infrastructure in their financial institutions and corporations. However, financial experts are discovering that, within the past few years, banks in the region have lost approximately 3.5 billion dollars to cybercrime.[16] More than 85% of banks in the West African region have reportedly been victim to atleast one cyberattack resulting in losses.[17]

The effectiveness of the legal frameworks in this sector largely depends on whether there is harmonisation across the domestic laws at the regional level. Domestic laws by themselves are insufficient. Cross-country co-operation is necessary to deal with a borderless problem such as cybercrime.[18] At a glance, it appears that this harmonisation is not at all present in Africa as far as normative and policy frameworks are concerned. Some of the approaches that have been taken by individual countries prove to be problematic when observed from a transnational perspective, resulting in disputes regarding cross-border arrests, prosecutions and punishment where any co-operative process has been pursued at all.[19]

While there have been efforts within most international and regional organisations to encourage cybersecurity awareness, there has not been any indication of a regional effort that is driven by the African Union (AU) to address the problem of cybercrime. The only document at AU level is the Convention on Cybersecurity and Personal Data Protection, which was adopted in 2014 as part of Agenda 2063.[20] At the time of writing, 14 States had signed and only 7 had ratified it.[21] Interpol's Africa Working Party on Information Technology has been advocating harmonisation of national legal frameworks by trying to

14 Gumbi (2018) at 54.
15 Corrigan (2020) at 7.
16 Odonkor (2020) at 1.
17 Olowu (2012) at 6; Berrada (2020) at 1.
18 UNCTAD (2013) at 5.
19 Olowu (2009) at 12.
20 Turianskyi (2018) at 15.
21 Turianskyi (2020) at 8.

persuade African countries to sign and ratify the Council of Europe Convention on Cybercrime (Budapest Convention).[22] To date, South Africa and Senegal remain the only African countries to have signed the Convention. Senegal has gone a step further than South Africa by ratifying the Convention, which entered into force in Senegal on 1 April 2017.

As far as international and regional efforts to combat cybercrime are concerned, Africa remains an insignificant actor, despite its increased vulnerability to cybercrime. There is an obvious apathy amongst African leaders to engage critically with cybercrime, which possibly might be due to the belief that the threat is not as real as it presents itself in the West. Turianskyi advocates that the AU should take lessons from the European Union (EU) when developing its cyber strategies whilst also being cognisant of the social, economic and geopolitical differences between the two.[23]

Accenture noted that South Africa faced a cross- industry spike in cyber-attacks in 2019. It is noted that there has been a 22 per cent increase in malware attacks in the first quarter of 2019 compared to the rate of the first quarter of 2018. This, it noted, amounted to an average of 577 attacks per hour.[24]

In 2019 alone, the country experienced attacks on Energy Supplier Eskom,[25] the South African Civil Aviation Authority,[26] CityPower,[27] Garmin South Africa,[28] Cool Ideas (South Africa's largest Internet Service Provider),[29] City of Johannesburg,[30] and a number of large banks including ABSA and Standard Bank,[31]

South Africa is an attractive target for cyberattacks because of various reasons which include a lack in cybersecurity investment, lack of law enforcement training and poor public knowledge of cyberattacks.[32]

22 Olowu (2009) at 11; Turianskyi (2020) at 7.
23 Turiansky (2020) at 6 -7.
24 Mcanyana, Brindly & Seedat (2020) at 4.
25 Abrams (2019) at 1.
26 Smith (2019) at 1.
27 Cimpanu (2019) at 1.
28 Gatlan (2019) at 1.
29 Cimpanu (2019b) at 1.
30 Cimpanu (2019c) at 1; Kaufmann (2021) at 1.
31 Kaufmann (2021) at 1.
32 Mcanyana, Brindly & Seedat (2020) at 4.

In a survey conducted by Stander in 2009,[33] it was found that 45 per cent of South African respondents reported that they had experienced one or more electronic attacks during the preceding 12 months. The respondents suspected that the most common motives for the electronic attacks on the integrity, confidentiality and availability of systems were foreign government political advantage (28 per cent), illicit financial gain (25 per cent) and indiscriminate random acts (22 per cent).[34]

It was estimated from data provided by the respondents that in the 12-month survey period, losses amounted to some R57.8 million, with R50.1 million of this total being lost through unauthorised access to information by insiders.[35] These are rough estimates, given the low rates of reporting of computer-related crimes. Thirty per cent of South African organisations chose not to report these crimes to anyone outside the organisation or to law enforcement. In the United States, 30 per cent and in Australia 69 per cent of organisations chose not to report such crimes. When asked why this was the case, 23 per cent of respondents in South Africa noted that they reported the attacks to legal counsel for civil remedies. Thirty-three per cent of respondents in South Africa indicated that they did not report the incidents because they believed that civil remedies would yield better results than criminal prosecution. Also, 27 per cent of the respondents were of the opinion that law enforcement would not be capable of apprehending the perpetrator and a further 27 per cent considered that the incident was not serious enough to warrant criminal reporting.[36] Only 15 per cent of South African respondents reported that the investigation resulted in charges being laid.[37]

In the first 72 hours of 2012, South Africa's state-owned Postbank suffered a devastating cyber-attack which resulted in R42 million being stolen by the cyberthieves. This hack was, at the time, one of the most sophisticated, visible and high-profile hacks witnessed in Africa. The cyberthieves were able to gain access to Postbank's servers through

33 Admittedly, this survey is more than a decade old but it used here for illustrative and comparative reasons rather than statistical contemporariness. Given the continued proliferation of cyberattacks in South Africa, there is no indication that the statistics have shown a marked improvement in recent years.

34 Stander (2009) at 223.

35 Stander (2009) at 224.

36 Stander (2009) at 224.

37 Stander (2009) at 225.

the compromised computer of an employee. Having done so, they proceeded to set up new accounts into which they could make fraudulent deposits. They then increased the withdrawal limits on these accounts and made withdrawals of large amounts from ATMs across the country.[38] Postbank holds over R4 billion in deposits and it is the entity through which millions of Rands in social grants move every month. A senior IT and banking security expert responded to the hack by stating that the Postbank network and security systems "are shocking and in desperate need of an overhaul". He added: "This [theft] was always going to be a very real possibility."[39] It has been reported that this heist came only three years after Postbank had spent in excess of R15 million on security upgrades to its fraud detection system.[40]

These statistics are not unique to South Africa. The study done by Stander was a comparative one, with data also from the United States and Australia. The statistics indicate the seriousness of cybercrime. Many states have taken measures to address it. For example, in November 2015, the United Kingdom announced the creation of the National Cyber Security Centre (NCSC) that would be the authoritative voice in information security in the UK.[41] South Africa has responded with a Cybercrimes Act[42] as its primary legislative measure to deal with cybercrime.

1.2 Understanding Cybercrime

The problems embedded in the issue of cybercrime are at least twofold. Firstly, the proliferation of cybercrime globally, and more specifically in South Africa, is outstripping the pace at which governments and lawmakers are able to respond efficiently. Secondly, where governments do manage to respond, there is a temptation to do so on the basis of a superficial understanding of the essence of cybercrime.[43]

---

38 Liebowitz (2012) at 1.
39 Sunday Times (2012) at 1.
40 Sunday Times (2012) at 1.
41 Gov.UK Press Release (2016) at 1; See the official NCSC website at https://www.ncsc.gov.uk/.
42 The Cybercrimes Act 19 of 2020 was signed into law by the President on 26 may 2021. All references to the Cybercrimes Bill refers to version [B 6B-2017]. The first version of the Cybercrimes Bill originally called the Cybercrimes and Cybersecurity Bill introduced in 2015 is referred to as Bill [B-2015]. The subsequent version passed by the National Assembly in 2018 is referred to as Bill [B6-2017].
43 Finlay & Payne (2019) at 1.

The main question that this study wants to answer is whether there are certain parameters that can be set in determining what constitutes cybercrime? In other words, given the complexity of cybercrime, is it possible to outline a threshold for the kinds of acts which would and which would not qualify as true cybercrimes[44] in order to determine which ought to have been included in the Cybercrimes Act?

There are a number of conceptual challenges that present themselves in the cybercrime context, but the one that is at the foreground of most discussions concerns the term "cybercrime" itself. The Council of Europe (CoE) has opted to describe various elements that make up cybercrime rather than offering a single definition. It has stated that cybercrime involves:

> action directed against confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data.[45]

This is an approach with which writers and law drafters are comfortable. However, a universally accepted scholarly definition of cybercrime yet is to be formulated.

What is more, the emergence of new terminologies, innovative tools and fresh dimensions to cybercrime continue to sow confusion. The development of cybercrime and the motivations that accompany it mean that the challenges transcend the traditional viruses and Trojans that once were predictable and controllable. In the early stages of the evolution of cybercrime, only a select few were capable of actually creating malware and thereafter the mischief typically would be committed by irresponsible hackers and script kiddies[46] for enjoyment.[47] Today, the landscape has shifted radically and cybercrime has become a massive industry which enjoys the support of organised criminal groups operating on a global scale. [48] Phishing and spam emails are amongst the major drivers of this criminal empire and while they may be effective cybercrime tools in their own right, they are supported by a plethora of crimeware[49] which develops at exponential rates.

---

44 The term "true cybercrimes" is used in this study in a specific technical sense as described in §3.3 below. Briefly, it refers to Type I cybercrimes which are cyber-dependent and violate the CIA triad.

45 Preamble to the Budapest Convention (2001) at 3.

46 "Script kiddies" is an informal term used to describe a person who hacks computer systems with code written by other people as they lacks the expertise to write his own.

47 Hajizadeh, Phan & Bauschert (2018) at 3. .

48 Lininger & Dean (2005) at 7, Wadhwa & Arora (2017) at 2219.

49 Wadhwa & Neerja (2017) at 2218, See Graham & Triplett (2016).

This shifting landscape of cybercrime needs to be assessed from various angles, which ought to include the motivations of the offenders. However, the Routine Activities Theory (RAT), the philosophy upon which this research is premised, takes it as a given that offenders have the inclination to commit crimes. It posits that there is no need to look at why a person offends and that what is important to investigate are the factors that allow said person to commit offences. The motivations of offenders therefore fall beyond the scope of this research. Still, it is important to note that motivations of offenders play a significant role in the ever-changing cybercrime terrain and therefore should not be ignored. Indeed, if these motivations are known, it may become easier to keep up with the trends and tools available to cybercriminals.

While cybercrime may not have a settled definition, the word itself has gained considerable popularity. This has resulted in other words, such as phishing and spam, entering the vocabulary of ordinary people. These are words that used to be the preserve of technical practitioners. Their adoption into the lexicon of every internet user is due largely to the explosive nature of this new mode of fraud.[50] Other crimeware, such as Trojan horses, spyware and bots, are integral to the cybercrime industry and they are bought and traded readily on the black market,[51] typically on the Dark Web. Their value lies in their deployment to steal sensitive data, such as banking details and credit card particulars, which can be exploited for financial gain without detection by the victim.[52]

The definitional complexities enveloping cybercrime are not limited to the theoretical sphere. Practitioners are confronted with the very real question of where exactly cybercrime occurs. From that question arises the question of what or where is cyberspace? How does it relate to the terrestrial space? Does it even occupy the terrestrial sphere, is it tangible or intangible? Who controls it? Can it be controlled? Can it be destroyed? This uncertainty about cyberspace provides an indication of why it is difficult for states and law enforcement agencies to trace, apprehend and prosecute cyber offenders. Territoriality and jurisdictional issues long have proved troublesome in international and foreign law because of considerations of state sovereignty. It goes without saying that if clearly defined borders

50 Olowu (2009) at 3.
51 Olowu (2009) at 3; Wadhwa & Neerja (2017) at 2218
52 TataRao v Reddy (2019) at 73.

between states can prove difficult in law enforcement, combating cybercrime in the borderless environment of cyberspace can prove impossible. It is necessary, therefore, to rethink the current crime-fighting techniques and to engage critically with questions such as these. These issues will be addressed in Chapters Five and Six. The discussion of RAT in Chapter Two will expand on this problem and provide some guidance, by way of a consideration of the spatio-temporal character of cybercrime and target suitability, as to what cybercrime is and how to handle it.

1.3 Definitional Considerations

One of the biggest challenges in combating cybercrime is defining it. Hitherto, a generally accepted definition of cybercrime has not been formulated. This section will discuss the various definitional issues relating to cybercrime.

As a prelude to that discussion, it is worthwhile to clarify certain other fundamental terms. Article 1 of the Budapest Convention defines four concepts, all of which are relevant to this study: (a) computer system; (b) computer data; (c) service provider; and (d) traffic data. It was understood by the drafters that these definitions would not need to be copied *verbatim* into the domestic laws of states parties, provided that those laws cover these concepts in a manner which is consistent with the principles of the Convention and offer an equivalent framework for its implementation.[53]

Computer System

The Budapest Convention defines a *computer system* as:

> any device or group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data.[54]

Under the Convention, then, a computer system is any *device* which consists of hardware and software that has been developed for automatic processing of digital data. *Automatic* means without direct human intervention, and *processing of data* means that data in the computer system is operated by executing a *computer programme*, which is a set of instructions that can be carried out by the computer to achieve the intended result. A *computer* is usually made up of various devices, including the processor, the central

53 Budapest Convention, Explanatory Report at 5.
54 Article 1(a) of the Budapest Convention.

processing unit (CPU) and peripherals such as a printer, CD writer/reader or storage device. It may have input, output and storage facilities, and it can stand alone or be connected in a network with other devices.[55]

A *network* is an interconnection between two or more computer systems.[56] It may be geographically limited to a small area, as with local area networks (LANs), or may span a large area, as with wide area networks (WANs).[57] The *internet* is a global network consisting of many interconnected networks which all use the same protocols. There are other types of networks which may not be connected to the internet, but what is essential is that there should be data exchanged over the network one way or the other.[58]

The definition of a computer system in the Cybercrimes Act is essentially the same as that in the Budapest Convention.[59]

Computer Data

The Convention defines *computer data* as:

> any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function.[60]

This definition builds on the ISO definition of computer data.[61] It contains the terms "suitable for processing", which means that the data must be put in such a form that it can be processed directly by the computer system. The notion of computer data was introduced in order to make it clear that the Convention was concerned with electronic data or other directly processable forms of information. It is the data that is processed automatically that

---

55 Budapest Convention, Explanatory Report at 5.

56 Interconnections may be earthbound (for example, through wires or cables), wireless (for example, through radio, infrared, or satellite) or both.

57 LANs and WANs themselves may be interconnected.

58 Budapest Convention, Explanatory Report at 5.

59 Section 1 of the Cybercrimes Act provides that a "computer system" means—
(a) one computer; or
(b) two or more inter-connected or related computers, which allow these inter-connected or related computers to—
(i) exchange data or any other function with each other; or
(ii) exchange data or any other function with another computer or a computer system.

60 Article 1(b) of the Budapest Convention.

61 According to the ISO definition, contained in ISO/IEC 2382-1: 1993, data is "a reinterpretable representation of information in a formalised manner suitable for communication, interpretation, or processing".

may be the target of one of the criminal offences defined in the Convention as well as the object of an investigation under the Convention.[62]

The Cybercrimes Act does not define computer data as a single concept; instead it defines each of its terms separately. Thus, it provides that "computer" means:

> any electronic programmable device used, whether by itself or as part of a computer system or any other device or equipment, or any part thereof, to perform predetermined arithmetic, logical, routing, processing or storage operations in accordance with set instructions and includes any data, computer programme or computer data storage medium that are related to, connected with or used with such a device.[63]

It goes on to define "data" as "electronic representations of information in any form" and a "data message" as "data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form".[64]

When read together, these discrete definitions capture the essence of what computer data is. As noted above, it was not the intention of the drafters of the Budapest Convention that domestic legislatures adopt these definitions *verbatim.* All that matters is that they capture the significant portions so as to make them as effective as they can be.

Service Provider

In the Budapest Convention, a *service provider* is:

> (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
> (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.[65]

The term is used to describe a broad category of persons playing a particular role in the communication or processing of data on computer systems. The first part of the definition makes it clear that both private and public entities are included if they provide users with the ability to communicate with one another. It therefore is irrelevant whether the users form part of a closed group (such as employees of a private enterprise to whom the service

62 Budapest Convention, Explanatory Report at 5.
63 Section 1 of the Cybercrimes Act.
64 Section 1 of the Cybercrimes Act.
65 Article 1(c) of the Budapest Convention.

is offered by a corporate network), whether the provider offers its services to the public, whether the services are offered free of charge, or whether they come at a fee.[66]

In the second part of the definition it is made clear that the term "service provider" applies also to entities which store or process data on behalf of service providers, as well as those entities which store or process data on behalf of the users of service providers. In terms of this definition, a service provider can be one who provides hosting or caching services, as well as one who provides a connection to a network. However, a mere provider of content, such as one who contracts with a web hosting company to host her website, is not intended to be covered by this definition if she does not also offer communication or related data processing services.

The Cybercrimes Act defines an "electronic communications service provider" to mean:

> any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act.[67]

The Electronic Communications and Transactions Act defines "electronic communications" as:

> the emission, transmission or reception of information, including without limitation, voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetism, radio or other electromagnetic waves, optical, electro-magnetic systems or any agency of a like nature, whether with or without the aid of tangible conduct, but does not include content service.[68]

It records also that an "electronic communications service" is:

> any service provided to the public, sections of the public, the State, or the subscribers to such service, which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services.[69]

These definitions are very broad and may not be adequate to address issues related to cybercrime. It is a missed opportunity by the drafters of the Cybercrimes Act not to have

66 Budapest Convention, Explanatory Report at 6.
67 Section 1 of the Cybercrimes Act.
68 Section 1 of the Electronic Communications Act 36 of 2005.
69 Section 1 of the Electronic Communications Act 36 of 2005.

defined an “internet service provider” in a way that is specific to addressing cybercrime because, as will be shown in §6.3.2 below, such providers play an important role in combating cybercrime.

Traffic Data

Under the Budapest Convention, “traffic data” refers to:

> any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.[70]

The term does not refer to the main communication itself, but rather to the data that is generated by computers in the chain of communication in order to route a communication from its origin to its destination. Therefore, this traffic data is auxiliary to the communication itself.

Traffic data is essential to investigations into criminal offences, as it is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence pertaining to the offence. Given that traffic data lasts only for a short period of time, it is necessary that its preservation be done expeditiously. Therefore, the ordinary procedures for collecting and disclosing computer data may be insufficient to deal with traffic data. It is the rapid disclosure of the data which is necessary to discern the route of the communication, so as to collect the relevant data before it is deleted or destroyed. In principle, the collection of this data may be regarded as being relatively unintrusive, since it does not reveal the content of the communication which generally is regarded as being particularly sensitive.[71]

While the Convention lists exhaustively the categories of traffic data that are treated by a specific regime, not all the categories may be available technically, capable of being produced by a service provider, or necessary for a particular criminal investigation. National legislators are at liberty to introduce differentiation regarding the legal protection of traffic data in accordance with its sensitivity. They are obligated to provide conditions and

70 Article 1(d) of the Budapest Convention.
71 Budapest Convention, Explanatory Report at 6.

safeguards which give adequate protection to human rights and liberties.[72] Traffic data is defined similarly in the Cybercrimes Act.[73]

While it might be almost impossible to have a single definition of cybercrime, the definition of key terms in the Convention provides a foundation upon which to build. National legislators can produce their own definitions which would be tailored to their unique needs. It is a delicate balancing act between having overly broad or overly narrow definitions which risk making the instruments ineffective.

1.4 International Dimension of Cybercrime

Cybercrime often has an international or transnational dimension to it. Much has been said about the threats posed by cybercrime and while the past twenty years have seen some improvements[74] there is still a long way to go. Ex-secretary general of the International Telecommunication Union (ITU), Mr Hamdoun Toure has been quoted as saying "at the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity".[75] Policy makers should focus on increasing public awareness about cybersecurity challenges and seek to strengthen regulatory and enforcement capabilities.[76] This is as true for Africa as it is for the rest of the international community. One weak link threatens the rest.

Since South Africa is a signatory to the Budapest Convention,[77] it becomes necessary to draw on the document as the overarching international authority on cybercrime legislation. As will be seen below, there are a number of similarities between the Convention and the South African Cybercrimes Act.

The explanatory notes to the Budapest Convention record that the Convention aims principally at: (1) harmonisation of the domestic criminal substantive law elements of offences in the area of cybercrime; (2) providing for domestic criminal procedural law

72 Budapest Convention, Explanatory Report at 6.
73 Section 1 of the Cybercrimes Act provides that "traffic data" means "data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type, of the underlying service".
74 See Kshetri (2019) at 79.
75 Kshetri (2019) at 77.
76 Kshetri (2019) at 80.
77 However, South Africa has not ratified the Convention yet.

powers which would be necessary for the investigation and prosecution of cybercrime offences; and (3) setting up a fast and effective regime for international co-operation.[78]

The Budapest Convention was promulgated in 2001. It is organised into four chapters which traverse: (I) Use of terms; (II) Measures to be taken at the domestic national level; (III) International co-operation; and (IV) Final provisions. Its preamble provides that the members of the Council of Europe and the other states signatory to the Convention recognise the value of fostering co-operation with other states parties, and that they are:

> convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation.[79]

The preamble also expresses a concern over the risk that computer networks and electronic information may be used to commit crimes and that the evidence which relates to such offences may be stored and transferred by computer networks which have undergone profound changes. These changes have been brought about by the digitalisation, convergence and continuing globalisation of these computer networks.[80] Furthermore, in order for the fight against cybercrime to be effective, increased, rapid and well-functioning international co-operation in criminal matters is necessary.[81] Importantly, the Convention is mindful of the need to ensure a proper balance between the interests of law enforcement and the respect for fundamental human rights as enshrined in a number of international instruments.[82] These instruments reaffirm:

> the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy.[83]

The Budapest Convention leans heavily towards international co-operation, more so than the Cybercrimes Act. The long title of the Act states only that:

---

78 Budapest Convention, Explanatory Report at 4.

79 Preamble to the Budapest Convention, para 4.

80 Preamble to the Budapest Convention, para 5.

81 Preamble to the Budapest Convention, para 8.

82 These include the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms; the 1966 United Nations International Covenant on Civil and Political Rights; the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and other applicable international human rights treaties. See Preamble to the Budapest Convention, paras 10 – 11.

83 Preamble to the Budapest Convention, para 10.

> the Executive may enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes.

This is not surprising in a piece of domestic legislation. However, more could have been said about the forms of international co-operation, as cybercrime would pose different challenges when compared to conventional crimes. This matter is discussed further in §5.3 below.

1.5 Literature and Statute Review

As noted above, the Cybercrimes Act represents South Africa's attempt to formulate a comprehensive legislative response to cybercrime. This Act, however, is not the first piece of South African legislation aimed at tackling the problem of cybercrime.[84] In 2002 already, the Electronic Communication and Transactions Act (ECTA)[85] was enacted to "provide for the facilitation of electronic communication and transactions" and "to provide for the development of a national e-strategy for the Republic".[86] The focus of ECTA is upon protecting "data" (electronic communication) and data messages.[87]

Cassim notes that before the commencement of ECTA, the relevant extant statutory law and the common law were applied to online forms of certain offences, for instance, indecency could be applied to child pornography, fraud could be used in cases of cyber fraud and *crimen injuria* was available to prosecute cyber smearing.[88] Prior to the enactment of ECTA, child pornography, for example, could be prosecuted under sections

84 As already stated, there is a dearth of literature available on the question of cybercrime in South Africa. The little that is there is relatively old and some which are more contemporary, do not address the issues sought to be answered by this study. Pause to note, the research undertaken by Pokwana & Kyobo (2016) which takes the view that the existing legislation governing the use of Information and Communications Technology that have been passed in South Africa are largely incoherent and misaligned. In that estimation, they consider the Electronic Communications and Transactions Act 25 of 2002, the Promotion of access to Information Act 2 of 2000, the Protection of Personal Information Act 4 of 2013, the Regulation on Interception of Communication Related Information Act 70 of 2002 and the Protection of State Information Bill 6 of 2010. Interestingly enough, even though that article was written in 2016 where the first draft of the Cybercrimes Act had already been circulated, it did not consider it. Kyobo went on to co-author another paper with Chigada (2018) and there too, the Cybercrimes Bill as it then was, was not discussed. The articles are worth noting and reading but, although contemporary, do not meet the concerns raised in this study and as such, will not be taken further.

85 Act 25 of 2002.

86 Long Title of ECTA.

87 Cassim (2010) at 118.

88 Cassim (2010) at 118.

27(1) and 28 of the Films and Publications Act.[89] However, there were certain computer related offences that could not be addressed adequately by the existing law, such as cyber theft, cyber extortion,[90] spamming[91] and phishing.[92] Chapter XIII of ECTA, spanning sections 85 to 89, provides specifically for cybercrimes. Sections 85(3) and 85(4) introduce new law relating to anti-hacking and anti-cracking by making it an offence unlawfully to:

> produce, sell, offer to sell, procure for use, design, adapt for use, distribute or possess or utilise any device … which is designed to primarily overcome security measures for the protection of data.[93]

Section 86 prohibits access to, interception of or interference with data. (Distributed) Denial of Service (DDoS) attacks are dealt with in section 86(5), and section 87 addresses the crimes relating to fraud, forgery and extortion. Spamming is prohibited in terms of section 45 of ECTA.

ECTA took the first steps in the confrontation with cybercrime, but its purpose was never to legislate for cybercrime in South Africa. Furthermore, despite the provisions of ECTA, the conversation regarding cybercrime never gained momentum outside cybersecurity professional circles. Certainly, cybercrime was seldom a concern of the academy in South Africa. This study therefore is both significant and timely in its anticipation of the newly enacted Cybercrimes Act.

South Africa has a serious deficit of legal and academic literature dedicated to the challenges posed by cybercrime. Nevertheless, discussion of the problem has gained some attention amongst cybersecurity and ICT experts. Writers such as Grobler & Dlamini have presented empirical data that highlight the extent of cybercrime in South Africa and thereby

89 Films and Publications Act 65 of 1996.

90 The most common tool for extortion currently is ransomware which entails the cybercriminal loading malware onto the victim's computer to encrypt it, making it inaccessible to the victim. The cybercriminal thereafter holds the computer data "hostage" and requires the victim to pay ransom (usually in cryptocurrency) in exchange for the decryption key.

91 Spamming means the despatch of irrelevant or unsolicited messages over the internet, typically through emails, with the intention of spreading malicious software (malware) or advertising or of launching a phishing attack.

92 Phishing occurs when a perpetrator sends fictitious emails to individuals containing links to fraudulent websites that appear official, with the intention of tricking the victim into revealing personal information, such as passwords, to the perpetrator.

93 Section 85(4) of ECTA.

have provided valuable statistics which confirm the existence of a serious problem that needs immediate attention.

In a study detailing global cyber trends, Grobler & Dlamini describe the reality of cybersecurity vulnerability in South Africa. For example, they find that, in terms of phishing attacks, South Africa ranked as one of the most attacked countries in the world.[94] In South Africa, the little literature that is available on cybercrime commonly is produced by the science and technology industry or is written from a business perspective. Be that as it may, it is from them that we are able to determine that cybercrime should be a legitimate concern.[95] Unfortunately, there is a great shortage of legal literature which deals specifically with cybercrime and how legislation should respond to it. This study seeks to etch a new path in the law through its critique of the Cybercrimes Act.

The Cybercrimes Act is the first piece of legislation to purport to offer a comprehensive solution to cybercrime in South Africa. Before its drafting, the little law pertaining to cybercrime was fragmented and relied upon the amendment of certain statutes to incorporate cybercrime elements. Snail discusses some examples of statutes that are applicable in the prosecution of cybercrime, including the Prevention of Organised Crime Act (POCA)[96] and the Financial Intelligence Centre Act (FICA).[97] These Acts merely have extended the prohibitions against the crimes which they governed to the cyber environment. So, for example, the prohibition against organised crime was applied automatically to any organised crime-related activities that may manifest in a "cyber" way. The same method was applied to offences relating to money laundering and other financial crimes that may be in contravention of the Exchange Control Regulations.[98]

The advent of ECTA was noted by Cassim and Snail as a great step towards addressing cybercrime in South Africa, but although it was very progressive, there was a lot of room for improvement. Cassim submits that for South Africa to protect itself against international cybercrime, it needs to ratify the Budapest Convention.[99] She is correct to

94 Grobler & Dlamini (2013) at 1.
95 Some examples of literature on cybercrime and cybersecurity are: Bougaardt & Kyobe (2011); Kyobe (2009); Herselman & Warren (2004); Kritzinger & Von Solms (2010); Burton & Mutongwizo (2009).
96 Act 121 of 1998.
97 Act 38 of 2001.
98 Snail (2009) at 7.
99 Cassim (2010) at 123.

emphasise the benefits for South Africa of ratifying the Budapest Convention, particularly since the country was involved in its drafting as a non-EU member. Also, South Africa has adopted certain elements of the Convention, for example, establishing a 24/7 point of contact. This study will explore the relationship between the Cybercrimes Act and the Budapest Convention more closely.

Cassim further suggests that there is a need for specialised cyber tribunals or courts that will facilitate the prosecution of cybercrime. This, she submits, has to be coupled with a balanced approach to the protection of fundamental human rights and the need for effective cybercrime prosecutions.[100] This is a view that is echoed by Snail, who commends South Africa for taking legislative steps in ECTA to deal with new crimes, although he remarks that these steps need to be scrutinised. In this regard, he maintains that the enforceability of the ECTA provisions still needs to be tested in the South African courts.[101]

Snail also applauds ECTA for having created some legal certainty about what constitutes cybercrime and what does not, noting that it does not preclude the application of any other statutory law or common law.[102] He observes that in the common law, some cyber activities could be criminalised by way of comparisons with and extrapolations of existing crimes. For example, the crime of breaking and entering with the intent to steal could be seen as a parallel to the cybercrimes of hacking and cracking. Similarly, the crime of malicious damage or injury to property could be analogous to the production and distribution of malicious code such as viruses, worms and Trojan horses.[103] In the case of *S v Howard*, the court confirmed that the crime of malicious damage to property could apply to conduct causing an entire system to break down through cyber means.[104] Snail sees this as confirmation that the crime of malicious damage to property was no longer limited to physical property, and could be applied to data messages and data information.[105] However, this view is incorrect because, as noted in the South African Law Reform Commission

100 Cassim (2010) at 123.
101 Snail (2009) at 11.
102 Snail (2009) at 6.
103 Snail (2009) at 3.
104 Unreported Case no 41/258/02, Johannesburg Regional Magistrates' Court.
105 Van der Merwe (2008) at 70.

(SALRC) study of 2001, malicious injury to property cannot be equated to any of the cybercrimes.[106]

The SALRC considered whether it had become necessary to create new offences to regulate certain cyber conduct, such as unauthorised access to computers and unauthorised modification of computer data and software applications. It compared malicious injury to property to these offences. Malicious injury to property is defined as "the unlawful intentional damage of another's property".[107] The elements of the crime are damage, property and culpability. Damage to property is caused when:

> property is destroyed, lost, permanently damaged or damaged to such an extent that it requires repair or that its use is permanently or temporarily interfered with.[108]

Furthermore, the damage that is caused to the property needs to be a consequence of the actions of the accused.[109] The SALRC noted that obtaining access to a computer, whether that access is authorised or not, does not cause any damage necessarily to the computer or even to the information that is stored on it. This circumstance, then, excludes the general application of the crime of malicious injury to property to the question of unauthorised access to a computer.[110] Of course, there are cases where unauthorised access or alteration to a computer or software system can cause damage to the information. In such cases the element of damage to property would be satisfied.

However, the second element of the crime requires that the damaged property be corporeal. A mere invasion of a person's economic domain is not sufficient to satisfy this element.[111] Hence, the cybercrime in question is disqualified as a version of malicious injury to property.[112] There does not appear to be any indication from the courts that they are considering extending the common law offence of malicious injury of property to cover the cybercrime of unauthorised access to a computer system, as it would require an extension of the concept of "property" to include intangible property.[113] Therefore, according to the

106 SALRC (2001) at 7.
107 Milton (1996) at 765.
108 Milton (1996) at 771.
109 Milton (1996) at 770.
110 SALRC (2001) at 5.
111 Milton (1996) at 771; Snyman (1992) at 545.
112 SALRC (2001) at 6.
113 SALRC (2001) at 6.

SALRC, the common law crime of malicious injury to property is inapplicable to the cybercrime of unauthorised computer access.

This conclusion by SALRC is correct and highlights an incorrect logic that some lawmakers apply to cybercrimes, namely, the logic that the common law can be transplanted simply into the cybercrime domain. This study, through a critique of the individual crimes in the Cybercrimes Act, proposes ways to classify cybercrimes so that they are not reduced to mere parallels of terrestrial crimes, as Snail tends to do. In addition, this study goes further than the SALRC report in that it will engage with all the crimes contained in the Act, whereas the SALRC report considers only the criminalisation of unauthorised access to computers and unauthorised modification of computer data or software.

Another piece of legislation which addresses certain elements of cybercrime is the Interception and Monitoring Prohibition Act (IMPA).[114] Section 86 of IMPA prohibits unauthorised access to, interception of or interference with data. It provides that anyone who intentionally and unlawfully accesses or intercepts any data without authority or permission is guilty of an offence.[115] IMPA was enacted in 1992 and was aimed specifically at governing the monitoring of transmissions, including emails. To this end, section 2 stipulates that no person shall:

> intentionally intercept or attempt to intercept or authorise, or procure any other person to intercept or to attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.

In simple terms, the section prohibits the intentional and unlawful monitoring or interception of data of any person, body or organisation. This includes attempt, which will be viewed as the actual act of unlawful interception. This prohibition, however, cannot be read to exclude any of the traditional justifications that will negate unlawfulness, such as private defence, necessity, court order or consent. Snail notes, though, that in the English case of *R v Secretary of State for Home Department, ex parte Rudduck and Others*,[116] the court gave notice that the grounds of justification should be used sparingly. In the case of unlawful interception, the court warned, the defence should not be available readily.[117]

114 Act 127 of 1992.
115 Section 86(1) of IMPA.
116 1987 (2) ALL ER 516.
117 Snail (2009) at 4.

From a reading of Snail's critique, he appears to be in favour of the strict construction regarding the grounds of justification, which is unfortunate because it prevents a critical engagement with the individual crimes and the justifications that the accused might have.

In a relatively new field such as cybercrime, it is ill-advised to perform a cursory adjudication of the elements of a cybercrime. Grounds of justification play an important role in this regard. Consider, for a moment, the case of two types of hackers, one called a *black hat* hacker and the other a *white hat* hacker. Both are hackers but their grounds of justifications are what set them apart. Black hat hackers are the nefarious kind of hackers, those who steal, cheat and destroy while white hat hackers are more benevolent than their black hat counterparts. Within the white hat category, there is a subset of hackers who are known as hacktivists (a term which is an amalgamation of hacker and activist). They are involved in social, political and economic activism and, depending on which side they support, they could be desired or undesired. Whilst hacking itself is a crime, the ground of justification plays an enormous role in the adjudication of the guilt of hackers or in determination of the sentences that should be imposed.

Snail argues also that a court's inherent right to develop the common law could allow it (automatically) to convict authors of viruses, worms and Trojan horses under the common law of malicious damage to property.[118] Unfortunately, this view entails a disproportionate extension of the exercise of judicial discretion. As noted in the SALRC report, such a development of the common law would not work readily.[119] Snail's opinion, although problematic, is representative of some of the problems besetting cybercrime. The nature of cybercrime does not allow for mere extrapolations of principles, where in some instances the judge will be liberal in her interpretation of an offence and in another instance be strict. The adjudication of cybercrime cannot be treated casually, particularly given the abundance of misinformation about it. The only way in which cybercrime can be combated successfully is by understanding it properly and ensuring that the principles used in its adjudication are not left to individual judicial discretion. In the absence of clear guidelines, efforts to combat cybercrime would be chaotic at best and unjust at worst.

118 Snail (2009) at 4.
119 SALRC (2001) at 12.

Snail and Cassim have commented on the strengths and shortcomings of ECTA and have concluded that while it may be imperfect, it is sufficiently progressive and has led to major legal developments in cybercrime discourse.[120] The introduction of the Cybercrimes Act may be seen as a continuation of South African efforts to formulate a comprehensive cybercrime framework. The question of how to deal with cybercrime in South Africa has been mooted through the various pieces of legislation discussed above. The Cybercrimes Act is the first piece of legislation that is dedicated to the regulation of cybercrime and promotion of cybersecurity in South Africa. This study continues from where the authors cited above have left off. As yet, there is little, if any, literature offering an encompassing critique of cybercrime in the context of the Cybercrimes Act. This study seeks to provide such a critique.

1.6 The International Historical Context

It is a widely held belief that there is a need for harmonisation of legal and technical solutions to the problem of cybercrime. Such harmonisation has been recognised by the international community, including states and supranational organisations, to be inherently transnational and borderless in nature. Some of the key participants in building international awareness and co-operation in this regard are the Council of Europe (CoE), the Organisation for Economic Co-operation and Development (OECD), the United Nations (UN), the European Union (EU) and the International Criminal Police Organisation (Interpol).[121] As the drivers of cybercrime awareness, they have set the tone for how states ought to respond.

The history of computer-related crime is as old as computers themselves.[122] According to Goodman & Brenner, there are four main waves in the development of national legislative responses to computer crime. The first wave of computer crime spanned the 1960s and 1970s, when computers themselves emerged. The first empirical study of computer crime occurred in the 1970s, with the publication of the first accounts of

120 Snail (2009) 11; Cassim (2010) at 123.

121 Goodman & Brenner (2002) at 37.

122 In this context, the words “computer crimes” and “cybercrimes” should not be used interchangeably because, just as computers have evolved significantly in the past half century, so have computer crimes.

computer crimes, including acts of espionage, computer manipulation, sabotage and the illegal use of computer systems.[123]

There were marked differences between the early computer crimes and modern cybercrimes, because yesteryear computers tended to be dedicated mainframes, that is, large, stand-alone machines and access to them usually required physical access to the terminals. They also were centralised mostly and not as interconnected as they are now. This meant that those who misused computer systems were more likely to be authorised users, for example, the computer technicians. It also meant that those who could manipulate the computers could do so up to the limit of their own talents and the nature of the computer systems themselves, unlike the script kiddies of today.

Prosecutors and judges were forced to tailor their prosecution and adjudication of these crimes to the existing laws related to theft, fraud, trespass, destruction of property and criminal mischief.[124] However, between the 1970s and the 1990s, major concerns were raised about privacy because of the emerging digital capabilities for vast collection, storage and transmission of data.[125] The legislative measures taken were not limited to the criminal law, but extended to administrative law and civil law in efforts to protect the privacy of citizens.[126]

In 1976, the United States Senate Committee on Homeland Security and Governmental Affairs held hearings on the need for computer crime legislation. In 1977, Senator Abraham Ribicoff introduced the Federal Computer Systems Protection Act as the first proposal for federal legislation regulating computer crime. The bill was revised and reintroduced in 1979. The bill died in committee, but it was the precursor to subsequent federal computer crime legislation.[127]

---

123 Sieber (1998) at §1.A.1.

124 Rasch (1995) at II.

125 Sieber (1998) at §I.A.I.

126 Countries which went this route included: Sweden (1973); the United States of America (1974); the Federal Republic of German (1977); Austria, Denmark, France and Norway (1978); Luxembourg (1979 and 1982); Iceland and Israel (1981); Australia and Canada (1982); the United Kingdom (1984); Finland (1987); Ireland, Japan and the Netherlands (1988); Portugal (1991); Belgium, Spain and Switzerland (1992); Spain (1995); and Italy and Greece (1997). This concern with privacy also prompted constitutional amendments in Brazil, the Netherlands, Portugal and Spain. See Sieber (1998) at §I.A.I.

127 See Kutz (1986) at 789 (Arizona enacted computer crime legislation in 1978).

The 1980s saw the second wave of computer-related law reform, which encompassed economic crimes. It was in the 1980s that hacking, viruses and worms began to emerge. Programme piracy, dispenser manipulation and telecommunication abuses also became more prevalent. Up to this point there was a great deficiency in the traditional law as it catered only for criminal acts that related to tangible objects. The new laws addressed the capabilities of computer systems to commit traditional crimes through new means, such as stealing money by manipulating bank accounts. They also dealt with intangible objects such computer programmes.[128]

The third wave of legislation also came in the 1980s, in the form of amendments and additions to national laws. This project was geared toward providing better protection for intellectual property by including copyright protection for computer programmes and the like.[129] The fourth wave was concerned with the regulation of illegal and harmful content on the internet. This campaign also emerged in the 1980s, but expanded significantly into the mid-1990s with the ubiquity of the internet. The content-related legislation focused on the regulation of pornography, the prevention of paedophilia, hate speech and defamation, and on the responsibilities of service and access providers.[130]

In the 1990s, the vulnerabilities of an information-based society, together with the limitations of the law and law enforcement efforts, were publicised widely. Today, cybercrimes extend far beyond their original ambit, ranging from financial crimes to attacks against national infrastructure, security and social well-being.[131] Furthermore, there have been a number of legal reforms since the 1970s in various countries (mostly European) that reflect the changes in both technology and legal paradigms. The criminal codes of old were focused on the protection of tangible objects, but as the information technology era

128 The following countries enacted legislation addressing computer-related computer crimes: Italy (1978); Australia (state law, 1979); United Kingdom (1981, 1990); United States of America (federal and state legislation in the 1980s); Canada and Denmark (1985); Federal Republic of Germany and Sweden (1986); Austria, Japan and Norway (1987); France and Greece (1988); Finland (1990, 1995); The Netherlands (1992); Luxembourg (1993); Switzerland (1994); Spain (1995); and Malaysia (1997). See Sieber (1998) at §I.B.

129 Sieber (1998) at §I.B.

130 Sieber (1998) at §I.B.

131 Sieber (1998) at §I.B.

advanced, society has placed great value upon incorporeal data, forcing legal systems to adapt and shift.[132]

1.7 Evolution of the South African Cybercrimes Act

Because South Africa is largely a consumer of technology rather than a producer, it has lagged behind in developing legislation and policies to address cybercrime and computer crime. It is not surprising that the first attempts to legislate this area were made in 2002 with the promulgation of the Electronic Communications and Transactions Act, as discussed in §1.5 above. Since then the, there has been much activity leading to the Cybercrimes Act being discussed here. It may well be that South Africa's development in this regard has been slow and staggered, but considering that the Budapest Convention was introduced only in 2001, South Africa's progress is apposite.

1.7.1 Long Titles of Bills [B—2015], [B6—2017], [B 6B—2017].

The Cybercrimes Act has undergone a number of changes since it first was presented for public comment in 2015.[133] Versions [B—2015] and [B6—2017] of the Bill were known as the Cybercrimes and Cybersecurity Bill, whereas version [B 6B—2017] was called the Cybercrimes Bill. The biggest difference between the various versions of the Cybercrimes Bill lies between [B—2015] and [B6—2017]. Version [B 6B—2017] merely solidifies the idea that there is a difference between cybercrime and cybersecurity matters by removing any aspects that deal with cybersecurity from the Bill, and recasting it as a dedicated cybercrimes Bill. It is [B 6B – 2017] that became the Cybercrimes Act 19 of 2020.

For the sake of good order, the long titles of the various versions of the Bill are recorded below:

- Version [B—2015]

  > to create offences and impose penalties which have a bearing on cybercrime; to further regulate jurisdiction of the courts; to further regulate the powers to investigate, search and access or seize; to further regulate aspects of international cooperation in respect of the investigation of cybercrime; to provide for the establishment of a 24/7 Point of Contact; to provide for the establishment of various structures to deal with cyber security; to regulate the identification and declaration of National Critical Information Infrastructures and measures to protect National Critical Information Infrastructures; to further regulate aspects

132 Sieber (1998) at §I.B.

133 The historical development of the Cybercrimes Act in this section will be discussed in the context of the Bills, noting that the [B 6B – 2017] culminated in the enactment of the Act.

relating to evidence; to impose obligations on electronic communications service providers regarding aspects which may impact on cyber security; to provide that the President may enter into agreements with foreign States to promote cybersecurity; to delete and amend certain provisions of certain laws; and to provide for matters connected therewith.

- Version [B6—2017]

  To create offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which is harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime; to provide for the establishment of a 24/7 Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes; to provide for the establishment of structures to promote cybersecurity and capacity building; to regulate the identification and declaration of critical information infrastructures and measures to protect critical information infrastructures; to provide that the Executive may enter into agreements with foreign States to promote cybersecurity; to delete and amend provisions of certain laws; and to provide for matters connected therewith.

- Version [B 6B—2017]

  To create offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which are harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of 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; to delete and amend provisions of certain laws; and to provide for matters connected therewith.

When compared to versions [B—2015] and [B6—2017] of the Cybercrimes Bill, version [B 6B—2017] shows a clear intention to streamline the purpose of the Cybercrimes Bill. The principle purpose of the Cybercrimes Bill, evident from each of the versions, is to create offences and impose penalties which have a bearing on cybercrime. Versions [B6—2017] and [B6 B—2017] go further than version [B—2015] by explicitly referring to the objective of criminalising the distribution of data messages which are harmful and providing for interim protection orders for victims while criminal proceedings are ongoing. This — the criminalisation of the distribution of harmful data messages —is the only offence which is embedded expressly in the long title. The offence is captured in the body of each of the versions of the Bill. In version [B—2015] it is contained under the offences heading in chapter 2 whereas in version [B6—2017] it is to be found in Chapter 3 under the malicious

communication heading. In version [B 6B—2017] it is found in Part II of Chapter 2 under the same heading of malicious communication.

It is argued later in Chapter 4 of this study that malicious communications should not be incorporated in cybercrime legislation because they constitute what is referred to as Type II cybercrimes which are computer enabled offences and thus not true cybercrimes. The long titles rather should have expressed an intention to criminalise hacking offences, such as unauthorised access to computer systems, which are argued to be true cybercrimes.

Each of the versions seeks to regulate jurisdiction. Version [B—2015] deals with the jurisdiction of the courts specifically, whereas versions [B6—2017] and [B6 B—2017] speak of jurisdiction generally. Versions [B6—2017] and [B6 B—2017] also go further than version [B—2015] by referring to a need to regulate aspects relating to mutual assistance in respect of the investigation of cybercrime.

Further, version [B—2015] empowers the President of the Republic to enter into any agreements with foreign states to promote cybersecurity. Version [B6—2017] vests that power in the Executive rather than the President. Presumably, this is to create more transparency and accountability in the kinds of agreements that may be concluded. It is worth noting that in version [B6—2017], the kinds of agreements that were being referred to were those pertaining to cybersecurity, even though it was already clear that that version was moving towards addressing cybercrimes and not cybersecurity. The same is true of the reference to critical information infrastructure. Version [B 6B—2017] definitively makes it clear that any agreements entered into by the Executive would be to promote measures which would aimed at detecting, preventing, mitigating and investigating cybercrimes.

Finally, both versions [B—2015] and [B6—2017] provide for the establishment of the 24/7 point of contact, whereas version [B 6B—2017] refers to it as the Designated Point of Contact. Apart from a few minor details, the two structures perform essentially the same functions.

These are just some of the aims provided for in the respective long titles, which give an indication of what one can expect in the various versions of the Cybercrimes Bill. The section which follows will engage further with some of the specific sections found in the Bills. The purpose of this exercise is not to provide an elaborate exploration of all the

provisions contained in versions [B—2015], [B6—2017] and [B 6B—2017] but rather to highlight some of the similarities and differences which are present.

1.7.2 Overview of Contents of Bills [B—2015], [B6—2017] and [B 6B—2017]

Version [B—2015] has 11 chapters and 68 sections, version [B6—2017] has 13 chapters and 63 sections and version [B 6B—2017] has 10 chapters and 60 sections.

In version [B—2015], all the offences are contained in Chapter 2. There are 20 offences in total.[134] These offences traverse a range of acts, which include personal and financial information related offences; unlawful access and interception of computer systems; computer-related fraud, forgery, extortion; espionage and terrorism; dissemination of harmful data messages and incitement; and infringement of copyright. The scope of version [B—2015] is exceptionally wide and it is hard to imagine how it would have been able to achieve what it had set out to achieve.

---

134 Chapter 2 of version [B—2015]: Offences
- Section 3: Personal information and financial information related offences
- Section 4: Unlawful access
- Section 5: Unlawful interception of data
- Section 6: Unlawful acts in respect of software or hardware tools
- Section 7: Unlawful interference with data
- Section 8: Unlawful interference with computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure
- Section 9: Unlawful acts in respect of malware
- Section 10: Unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices
- Section 11: Computer related fraud
- Section 12: Computer related forgery and uttering
- Section 13: Computer related appropriation
- Section 14: Computer related extortion
- Section 15: Computer related terrorist activity and related offences
- Section 16: Computer related espionage and unlawful access to restricted data
- Section 17: Prohibition on dissemination of data message which advocates, promotes or incites hate, discrimination or violence
- Section 18: Prohibition on incitement of violence and damage to property
- Section 19: Prohibited financial transactions
- Section 20: Infringement of copyright
- Section 21: Harbouring or concealing person who commits offence
- Section 22: Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring to commit offence

Version [B6—2017] has fewer offences which are contained in two chapters. Chapter 2 provides for 12 offences[135] and Chapter 3 for three offences.[136] The same is true of version [B 6B—2017] in which the offences are provided for in Part I and Part II of Chapter 2. Part I contains 11 offences,[137] while Part II records three offences.[138]

Each of the versions has a chapter on jurisdiction,[139] followed by a chapter on the powers to investigate, search and access or seize.[140] Apart from differences in wording, the

---

135 Chapter 2 of version [B6—2017]: Cybercrimes
- Section 2: Unlawful securing of access
- Section 3: Unlawful acquiring of data
- Section 4: Unlawful acts in respect of software or hardware tool
- Section 5: Unlawful interference with data or computer program
- Section 6: Unlawful interference with computer data storage medium or computer system
- Section 7: Unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices
- Section 8: Cyber fraud
- Section 9: Cyber forgery and uttering
- Section 10: Cyber extortion
- Section 11: Aggravated offences
- Section 12: Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence
- Section 13: Theft of [an] incorporeal

136 Chapter 3 of version [B6—2017]: Malicious Communications
- Section 16: Data message which incites damage to property or violence
- Section 17: Data message which is harmful
- Section 18: Distribution of data message of intimate image without consent

137 Chapter 2, Part I of version [B 6B—2017]: Cybercrimes
- Section 2: Unlawful access
- Section 3: Unlawful interception of data
- Section 4: Unlawful acts in respect of software or hardware tool
- Section 5: Unlawful interference with data or computer program
- Section 6: Unlawful interference with a computer data storage medium or computer system
- Section 7: Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device
- Section 8: Cyber fraud
- Section 9: Cyber forgery and uttering
- Section 10: Cyber extortion
- Section 11: Aggravated offences
- Section 12: Theft of incorporeal property

138 Chapter 2, Part II of version [B 6B—2017]: Malicious Communication
- Section 14: Data message which incites damage to property or violence
- Section 15: Data message which threatens persons with damage to property or violence
- Section 16: Distribution of data message of intimate image

139 Chapter 3 in version [B—2015], Chapter 4 in version [B6—2017] and Chapter 3 in version [B 6B—2017].

140 Chapter 4 in version [B—2015], Chapter 5 in version [B6—2017] and Chapter 4 in version [B 6B—2017].

substantive content of these provisions is similar. Versions [B6—2017] and [B 6B—2017] also have additional chapters which are not in version [B—2015], such as mutual assistance and the 24/7 or designated Points of Contact.

The issue of evidence is addressed in each of the versions of the Cybercrimes Bill but to varying degrees. Version [B—2015] provides for the general admissibility of affidavits and evidence. It also provides for the admissibility of evidence in the context of assisting and co-operating with foreign states. Versions [B6—2017] and [B 6B—2017] provide only for accepting proof of certain facts by affidavit.

The provisions on the admissibility of evidence found in section 63 of version [B—2015] would have been useful to retain in the latest version [B 6B—2017] version. Section 63 of version [B—2015] provides, amongst other things, that the rules of evidence should not be applied in such a way that they preclude the admissibility of data, a data message or data document (data) as evidence merely on the grounds that it is data.[141] Also, the best evidence that the person adducing it reasonably could be expected to obtain ought not to be precluded from admissibility on the grounds that it is not in its original form.[142] It further provides that evidence in the form of data must be given due evidentiary weight, subject to the evidence being assessed and due regard being had ~~for~~ to the reliability of the manner in which the data was generated, stored or communicated, as well as to the reliability of the manner in which the integrity was maintained.[143] What is more, if a copy or printout of data is produced with a declaration that it is authenticated in the prescribed manner, it may be admitted as rebuttable proof of the contents of such data.[144]

Those provisions of version [B—2015] were important because they would have allowed courts more flexibility in dealing with electronic data evidence. It is understood well that the rapidity with which events occur in cyberspace does not lend itself always to the preservation and retention of original evidence. If there were to be an insistence upon original evidence being made available at all times, it would be nearly impossible to prosecute and convict cybercriminals. By the same token, however, it is desirable that the legislation provides some safeguards to ensure that the evidence that is placed before the

141 Section 63(1)(a) of version [B—2015].
142 Section 63(1)(b) of version [B—2015].
143 Section 63(2)-(3) of version [B—2015].
144 Section 63(4) of version [B—2015].

courts is reliable. In the age of artificial intelligence, augmented reality and deep fakes, every measure must be taken to ensure that the evidence that is admitted in court is reliable. All in all, it is unfortunate that like evidentiary provisions did not make it into version [B 6B—2017].

Other provisions which did not survive from version [B—2015] into version [B 6B—2017] are the chapters that provide for structures to deal with cybersecurity[145] and national critical information infrastructures.[146] Version [B6—2017] retained these chapters, but with significant differences. For instance, where version [B—2015] provided for eight sections to create structures to deal with cybersecurity, version [B6—2017] only contained four, namely, the cyber response committee,[147] government structures supporting cybersecurity,[148] nodal points and private sector computer security incident response teams,[149] and information sharing.[150]

The interesting structure to note and which ought not to have been left out in version [B 6B – 2017] is the Computer Security Incident Response Teams (CSIRTs). CSIRTs are an essential ingredient of the protection of the economy and national critical infrastructure.[151] They usually operate on an *ad hoc* basis, but they are essential because they have the capacity to respond to incidents in a systematic manner.[152] CSIRTs perform a range of services, which include intrusion detection as the first tier of an incident response team. The CSIRT is poised best to analyse incidents quickly and accurately. It also may

145 Chapter 6 of version [B—2015]: Structures To Deal With Cybersecurity
Section 50: Definitions and interpretation
Section 51: Cyber Response Committee
Section 52: Cyber Security Centre
Section 53: Government Security Incident Response Teams
Section 54: National Cybercrime Centre
Section 55: Cyber Command
Section 56: Cyber Security Hub
Section 57: Private Sector Security Incident Response Teams

146 Chapter 7 of version [B—2015]: National Critical Information Infrastructure Protection
Section 58: Identification and declaring National Critical Information Infrastructures
Section 59: Establishment and control of National Critical Information Infrastructure Fund
Section 60: Auditing of National Critical Information Infrastructures to ensure compliance

147 Section 53 of [B6—2017].

148 Section 54 of version [B6—2017].

149 Section 55 of version [B6—2017].

150 Section 56 of version [B6—2017].

151 Van De Kleij, Kleinhuis & Young (2017) at 1.

152 Van De Kleij, Kleinhuis & Young (2017) at 2.

provide advisories to an organisation about new vulnerabilities and threats, supplementing the education and awareness services which the CSIRTs provide. The more technical expertise there is within an organisation, the easier it is to detect, report and respond to incidents and the less pressure there is or should be on an incident response team.[153]

CSIRTs play an important role in the fight against cybercrime and version [B 6B—2017] would have done well to incorporate provisions for their establishment in both the public and private sectors. One would have expected that they would have been included as part of the responsibilities of the Designated Point of Contact as the oversight body. Although version [B 6B—2017] does not provide for structures concerned with the protection of critical information infrastructures, it remains important to employ the functions of the CSIRTs because incidents are inevitable at every level of cybersecurity and cybercrime.

With regard to the chapter of on the protection of infrastructure, version [B6—2017] referred to *critical information infrastructure* as opposed to *national critical information infrastructure*.[154] It also did away with the section providing for the establishment of a National Critical Information Infrastructure fund.[155]

The provisions on critical information infrastructures spoke to the information infrastructures that are of such a strategic nature that any interference with them may jeopardise the security, defence, law enforcement or international relations of the Republic; prejudice the health and safety of the public; interfere with or disrupt essential services; cause major economic loss; destabilise the economy of the Republic; or create a public emergency situation.[156] Significantly, version [B 6B—2017] omits all mention of critical information infrastructures. However, this is not a mighty loss for the operation of the legislation, as it beyond the scope of the Cybercrimes Act and it most likely will be included in forthcoming cybersecurity legislation.

It is abundantly clear that the Cybercrimes Act has seen significant developments in becoming the legislation which this study seeks to analyse critically. At face value, the

153 Cichonski *et al* (2012) at 17.
154 Sections 57 and 58 of version [B6 B – 2017].
155 Section 59 of version version [B—2015].
156 Section 58(2) of version [B—2015].

evolution appears to have been for the better. However, a definitive determination of that assessment will emerge as the study unfolds. Version [B 6B – 2017] supersedes the earlier version of the Cybercrimes Bill to become the Cybercrimes Act 19 of 2020 and that is what study will deal with.

1.8 Outline of Remaining Chapters

The study will span five more chapters, as outlined below.

Chapter Two

This chapter will expound the philosophy underpinning the study. It will propose a two-part framework that will categorise and appraise cybercrime. The first part is the Gordon & Ford Classification (G&FC) of cybercrime and the second part is the Routine Activities Theory (RAT) as formulated by Cohen & Felson.

Chapter Three

This chapter, together with the next, will be dedicated to a comprehensive appraisal of the Cybercrimes Act. The chapter will deal with the offences provided for in Part I of Chapter 2 of the Cybercrimes Act. These are offences that are categorised as Type I cybercrimes according to the G&FC. Additionally, the chapter will focus on the first essential element of RAT, which is the motivated offender.

Chapter Four

This chapter will deal with the so-called Type II cybercrimes provided for in Part II of Chapter 2 of the Cybercrimes Act. It will consider also the second essential element of RAT, which is the suitable target.

Chapter Five

This chapter will deal briefly with the procedural aspects of the Cybercrimes Act by discussing jurisdiction, powers to investigate, search and access or seize, and mutual assistance.

Chapter Six

This chapter will assess South Africa's efforts to regulate cybercrime by focusing on the third essential element of RAT, which is the capable guardian in the form of the Designated Point of Contact (DPoC) as provided for in Chapter 6 of the Cybercrimes Act.

Chapter Seven

This chapter will bring the study to a close by providing answers to the research questions and making recommendations, if necessary, for improving the South African legislative response to cybercrime.

CHAPTER TWO

UNPACKING CYBERCRIME

2.1 Introduction

Cybercrime is being discussed more and more frequently across many different platforms, including academic journals, computer magazines, news outlets and online. It has gained much publicity and notoriety in popular culture, social media and lay discussions. While this kind of engagement has helped raise awareness of the threats of cybercrime and the challenges of cybersecurity, regrettably it has contributed to a certain confusion regarding the meaning of the problem and how best to deal with it.[1] The problem is exacerbated by the fact that there is no universally accepted definition of cybercrime. Research has shown that while the word "cybercrime" has entered into common usage, many people find it hard to define it precisely.[2]

The Cybercrimes Act does not provide a self-contained definition of cybercrime. Instead, it defines certain elements that make up the cybercriminal environment, such as what constitutes a computer device, what is data and what kind of conduct would be classified as access to a computer or network. Whether or not it is even desirable to have a single definition of cybercrime is a very contentious topic amongst academics and practitioners precisely because of the complexities that cybercrime presents. For example, a computer or device may be an agent of a crime, the facilitator of a crime or the target of a crime.[3] Furthermore, the crime can take place on the computer itself or it can take place in a different non-virtual location.[4] These kinds of variations may be difficult to capture in a blanket definition. Definitions differ depending on the perspective from which they are formulated, be it that of the observer/protector or the victim.[5] Thus, the Budapest Convention uses the term cybercrime to refer to offences which range from criminal activity against data to content and copyright. However, Zevier-Geese suggests that that definition

1 Gordon & Ford (2006) at 13.
2 Gordon & Ford (2006) at 13.
3 Azad, Mazid & Sharmin (2017) at 3.
4 Gordon & Ford (2006) at 14.
5 Gordon & Ford (2006) at 14.

is insufficient because it should include activities such as fraud, child pornography and cyberstalking.[6] Such definitional disagreements express the challenges embedded in the notion of cybercrime.

2.2 The Novelty of Cybercrime

One of the prominent questions concerning cybercrime is whether or not it is a new form of criminality. If it is, then analysts would be required to dispense with (or at least modify, supplement or extend) the existing theories of criminology. Unsurprisingly, there are varying answers to this question which appear with positive, negative and indeterminate registers.[7]

Certain commentators, such as Capeller, suggest that the advent of virtual crimes may present the beginning of a new and distinctive environment for criminality. The term "cyberspace" often is used as a contrast to "real space", as an environment that has its own ontological and epistemological structures, and that has different rules and interactional forms, as well as new limits and possibilities. This newness, she argues, may necessitate a new criminological vocabulary.[8] Others, such as Grabrosky, are sceptical of this proposition. He uses the analogy of "old wine in new skins" to describe the advent of the virtual crime era.[9] He proposes the Routine Activities Theory (RAT) as a way in which cybercrime may be explained and made to fit into the existing criminological theories, classifications and aetiological schema.[10]

This study takes the position that cybercrime is neither completely novel nor is it merely a virtual manifestation of the ordinary terrestrial crimes. As stated earlier, the premise of this research is that cybercrime is an interesting and unique form of criminality which manifests itself in a number of ways. These manifestations need to be considered independently and comprehensively if effective countermeasures are to be devised. This is not to say that every single offence has to be considered critically. That would be

6 Zeviar-Geese (1998).
7 Yar (2005a) at 407.
8 Yar (2005a) at 408.
9 Grabosky (2001) at 243. In a political context, there have been formal declarations by some states calling cyberspace the fifth domain of warfare – after land, sea, air and space. To this end, states have begun to conduct intelligence and pseudo-military operations in that domain. It is arguable whether these operations can be called "cyberwar" but indeed, they do create a state of "unpeace". See Broeders & van den Berg (2020) at 1.
10 Yar (2005a) at 408.

impracticable. It would suffice that certain types of cybercrimes be classified differently from other types, so as to not paint all with the same brush. The categorisation into types proposed by Gordon & Ford is particularly helpful in this regard and will be discussed in §2.3 below.

At this juncture, the work of Grabosky and Capeller requires further consideration. Grabosky begins his critique of cybercrime studies with the caution that we should be wary of overgeneralisations and hyperboles. He asserts that "virtual criminology" is, in essence, the same as the terrestrial crime with which we are familiar, although some of the manifestations may be new by virtue of the medium used.[11] The first justification for this assertion is that the motivations of offenders for committing crimes have not changed. Computer criminals are driven by the same time-honoured motivations, which range across greed, lust, revenge, power and adventure, culminating in the desire to taste "forbidden fruit". Greed is what primarily drives electronic fraud, while lust drives the creation and distribution of child pornography. Furthermore, given the technical competence needed to commit a number of cybercrimes, the intellectual challenge of mastering complex systems is another motivator. Grabosky observes that the only novel aspect of cybercrime is the unprecedented technological capacity — the motivations for cybercriminal conduct remain the same as for ordinary criminal conduct.[12] This observation may be accepted. Indeed, RAT takes the inclination to offend as a given, and therefore (as intimated earlier) the motivations of cybercriminals are beyond the scope of this research.

The rest of the critique by Grabosky, however, suffers from an important deficiency in that it fails to recognise different types of cybercrime. He appears to assume that there are only Type II crimes and neglects to consider Type I cybercrimes (in terms of the G&FC). More specifically, he focuses on computer- enabled crimes, making regular reference to cyber fraud, cyberstalking, online child pornography and child grooming. He makes the case that these crimes are different from ordinary crimes only as regards the scale on which they are committed and the higher level of difficulty they present to law enforcement efforts. Grabosky asserts that the greatest challenge of digital criminality lies in its enormous

11 Grabosky (2001) at 243.
12 Grabosky (2001) at 244.

potential for transnational offending.[13] However, he argues that even this does not create problems that the world is not facing already, such as the difficulty that comes with dual criminality. To illustrate his point, he refers to the "paradoxes of the digital age" which highlight the rise of technologies designed to provide anonymity and pseudonymity in relation to the ever-shrinking power of the state to direct and control internet traffic.[14]

Capeller begins her discussion of cybercrime by arguing that ICT is developing so intensely that the scientific community needs to revise its sociological, philosophical and historical assumptions. She refers to cyberspace as a reflection of a society of individuals in which there have been technological and cultural mutations that have made possible abstract worlds based on the "real world".[15] In general, she argues that there has to be a reconsideration of the criminological criteria as the current system is incapable of explaining the new forms of deviance making up cybercrime.[16] She asserts that virtual criminality no longer views cyberspace merely as a support system but that cybercriminals take advantage of the framework and context of cyberspace as it exists to offend.[17]

The first consideration in Capeller's argument is the relationship between trust and risk. Trust and risk are regarded to be dependent on the perceived reliability or stability of the cyberspace system rather than on how it functions in reality. In a sense, both trust and risk are connected to the uncertainty of the system.[18] This corresponds to a move from a welfare state to a risk society, the latter being defined as a:

> period in which social, political and ecological (individual or collective) risks, generated by the drive for renewal, increasingly escape society's control and security agencies.[19]

The claim is that contemporary society has transformed into a risk society in an unplanned manner and without proper precautions having been taken against possible repercussions and dangers.[20] Trust and risk are seen to form the basis of virtual interactions, in a new context referred to as "virtual risk". Such virtual risk may be observed in e-commerce,

13 Grabosky (2001) at 247.
14 Grabosky (2001) at 245.
15 Capeller (2001) at 229.
16 Capeller (2001) at 230.
17 Capeller (2001) at 231.
18 Capeller (2001) at 231.
19 Capeller (2001) at 232.
20 Beck (1994) at 334.

contracts, and protection of individual rights, and even in surfing "cyberdeviant spaces" such as the deep web.[21]

A second consideration is the problem presented by anonymity, which increases risk. Anonymity is one of the bigger challenges that comes with cyberspace. It is also one of the desirable features of the internet, with users being able to adopt a new *persona* relatively easily.[22] The non-linear, transnational and ever-changing character of the internet renders the possibilities of anonymity endless. Some argue that while anonymity should be protected, it also should be limited by law for purposes of accountability, the absence of which encourages lack of civility and offensive behaviour.[23] However, over the past few years there has been a growing trend towards greater internet anonymity. Capeller notes that the impact of anonymity is significant in an environment which is expanding continuously and has grown into a space that is available to the general public. The internet itself has evolved and the socialisation of cyberspace has created conditions that are favourable to the growth of illegal interactions, whether economic or not.[24]

Capeller captures the debate regarding the nature of cybercrime well in her proposition that:

> cybercrime is not only a *means* or a *support* for criminal action, it is a true *autonomous environment* in which systemic and abstract criminal actions are spreading.[25]

The questions of the relationship between trust and risk and of anonymity are indicators of the shift from mere support to a real environment. It therefore is essential to make the distinction between the notions of support and environment in order to be able to understand the new phenomenon of cybercrime.

The concept of support speaks to the idea that computers are mediums or tools through which illegal activity takes place or through which new types of crimes are

21 The terms "dark web" and "deep web" are used interchangeably in this study whilst noting the nuanced differences between the two. Typically, the deep web refers to the whole unindexed portion of the internet accessible through avenues such as The Onion Router (ToR), whereas the dark web typically refers to the grotesque underbelly of the deep web where nefarious activities such as violent child pornography is present.

22 See Moore (2018).

23 Capeller (2001) at 233.

24 Capeller (2001) at 234.

25 Capeller (2001) at 234 (original emphasis).

perpetrated. On the one hand, the internet can be seen as a sphere in which criminal techniques are disseminated and criminal recruitment takes place. On the other hand, the internet is an environment where real material frameworks have been created to foster a community constituted in terms of illegal, interactive and virtual actions. That the internet cannot be comprehended merely as a supporting context for crime is underpinned by its peculiar dynamism, as shown in how rapidly and intensely it transforms.[26] Furthermore, the fact that unlawful acts, techniques and innovations are transmitted in real time designates this new virtual criminal playing field. What is more, the field is very flexible and is not controlled centrally,[27] making it possible for financial transactions to be completed securely, without the involvement of any banks at all. Bitcoin is a prominent agent in this regard.[28]

Capeller makes a compelling argument for alternative thinking about cybercrime. If her position is accepted, it becomes evident that it indeed is necessary to adopt new and improved methods for combating cybercrime. Capeller's work supports the argument of this study, that cybercrime cannot be dealt with appropriately without a thorough understanding of its unique characteristics. It is important to note that her denotation of cyberspace as a criminal environment does not entail a dismissal of its properties as a support for terrestrial offences, such as computer enabled crimes. This means that existing knowledge can be useful still. In other words, cybercrime should not be viewed through one inflexible lens and countermeasures need to adapt to the many facets of cybercriminality.

Capeller's examination of cybercrime is preferable to that of Grabosky. She acknowledges the complexity of cybercrime, whereas Grabosky considers only one aspect of cybercrime and comes to a conclusion which may address only one form of cybercrime, at the expense of the rest.

2.3 The Gordon & Ford Categorisation of Cybercrime

Gordon & Ford propose categorising cybercrime into two basic forms, namely, Type I and Type II, with a view to foregrounding the breadth of the issue.[29] They find that it is common

26 Capeller (2001) at 234.
27 Capeller (2001) at 234.
28 See Nakamoto (2008); Ghimire & Selvaraj (2018).
29 Gordon & Ford (2006) at 14; this categorization has been adopted in other works such as Wadhwa & Neerja (2017) at 2217 – 2218.

for researchers to define the issue too narrowly, thereby limiting law enforcement capabilities. Their dual categorisation of cybercrime is designed to provide a conceptual framework within which lawmakers may create legal definitions which will vary across jurisdictions. This conceptual framework will be used in this dissertation in order to engage critically both the definition of cybercrime and the classification of cybercrimes adopted in the South African Cybercrimes Act.

Type I cybercrimes are technical in nature when compared to Type II cybercrimes. From the perspective of the victim, Type I cybercrimes are generally singular or discrete events that often are facilitated by introducing crimeware programmes into the victim's computer system. Examples of Type I cybercrimes include phishing attempts, identity or data theft, and e-commerce or banking fraud facilitated by stolen credentials.[30] Furthermore, these cybercrimes usually are facilitated through an exploitation of vulnerabilities in a computer system which allow for the introduction of crimeware. Preventing Type I cybercrimes therefore requires a significant "thought change" amongst the general population, because not only must citizens protect their data from traditional threats such as viruses and worms, but they need also to become aware of the concept of vulnerabilities.[31]

In Type I cybercrimes, crimeware is an important element because it is the malicious software (malware) that is introduced into a computer system to help the cybercriminal perpetrate the crimes. The installation of such crimeware is one of the elements that differentiates Type I cybercrimes from Type II cybercrimes. The crimeware can be used directly or indirectly in the commission of the crime. By definition, malware is undesirable from the perspective of the computer user. Gordon & Ford define crimeware as:

> software that is used (directly or indirectly) in the commission of a criminal act; and not generally regarded as a desirable software application from the perspective of the computer user and is not involuntarily enabling the crime.[32]

This definition of crimeware is a common one for the most part, and Gordon & Ford found it appropriate to go a step further by including an element which provides that the software is

30 Gordon & Ford (2006) at 14.
31 Gordon & Ford (2006) at 14.
32 Gordon & Ford (2006) at 17.

"not involuntarily enabling the crime".[33] This last element, formulated as a double negative, plays an important role by distinguishing between software that is inherently malicious and software that is taken over to commit a malicious act. For example, the fact that a browser has a vulnerability which is exploited by an attacker does not mean that the browser software itself is crimeware. It may be simply flawed software.[34]

The Kaspersky definition, like many others, limits the definition of crimeware to its being used in financial crimes. This is an approach that Gordon & Ford find problematic because the definition should not identify use for a specific type of cybercrime. This is an important consideration and highlights the definitional difficulties that surface with elements of cybercrime which may categorise a programme according to how it has been used rather than according to its content. Like cybercrime, crimeware occupies a broad spectrum, and if one uses a social media platform or IM (instant messaging) client to commit a cybercrime, that platform, application or client software itself may not be crimeware. Keystroke loggers, spyware, Trojan horses and bots are just some of the programmes that may be considered to be crimeware.[35] The failure to delineate carefully between legitimate software that is used to facilitate crimes and software whose sole purpose is to execute the crime adds much confusion. It is worth noting that software itself lacks "intent" and therefore it is up to the observer to try and ascertain the intention of the software programmer.[36]

Although navigating definitions in the context of cybercrime is a demanding exercise, it remains imperative to find definitions or descriptions that are progressive. What this means is that the definitions need to be broad enough to capture the essential elements while not being so broad as to lose their effectiveness. Gordon & Ford correctly state that crimeware should not be defined contextually because it results in these determinations being undecidable.[37] For instance, one cannot say that because the IM client was used to perpetrate the crime of cyberstalking in a particular context, therefore the IM client is a form of crimeware.

33 Gordon & Ford (2006) at 16.
34 Gordon & Ford (2006) at 16.
35 Gordon & Ford (2006) at 16, Wadhwa & Arora (2017) at 2218.
36 Gordon & Ford (2006) at 17.
37 Gordon & Ford (2006) at 16.

The following example illustrates a typical Type I cybercrime. Cassandra uses online banking and frequently shops online because she enjoys the convenience. She receives an email from her bank which informs her that it is updating its online banking software and it needs clients to verify their credentials. The email provides a link that she is requested to follow in order to complete the process. Cassandra, not suspecting any foul play, follows the link which sends her to the homepage of her bank. If Cassandra had been vigilant she would have noticed that the link which she followed was not identical to the one which the bank itself uses. The link takes her to a website that is actually a clone of the real website. However, it appears to be identical to the original site and, therefore, when Cassandra is prompted to type in her user identity and her password, she does so without hesitation. As she types in the details, they appear in plain text to the cybercriminal on the other side who copies them and uses them to gain access to her bank account. Cassandra completes the transaction without suspecting anything until her bank account is emptied three days later. This is what is known as a phishing scam. When it is viewed from Cassandra's (the victim's) perspective, it is, firstly, a singular and discrete event and, secondly, it involved the use of crimeware.

In terms of the discussion above regarding the definition of crimeware, the email client was used to deliver the spam email and, therefore, if interpreted strictly and contextually, the email facilitated the commission of a cybercrime, and could be incorrectly classified as crimeware. In this instance the real crimeware are the software that created the clone of the bank's site and the keylogger software that stole the username and password.

Type II cybercrimes exist on the other end of the cybercrime spectrum. They have a more pronounced human element to them.[38] They include, but are not limited to, cyberstalking and harassment, extortion and blackmail, child predation, complex corporate espionage and planning or perpetrating online terrorism. Type II cybercrimes usually are facilitated by the use of programmes, such as social media platforms, which would not be classified normally as crimeware. Furthermore, these crimes generally are repeated events from the perspective of the victim.

38 Gordon & Ford (2006) at 13.

Consider the following example. Amu and Basani meet in an online chatroom dedicated to sharing views about the current state of South African politics. Amu is very fascinated by the views that Basani presents and asks her to interact through a private chat. They exchange phone numbers and begin to chat privately. The conversations continue for some weeks and Amu begins to develop romantic feelings for Basani. He searches for her profile on a popular social media platform. He realises from her profile that she lives in the same town as he does and asks her out on a date at a local restaurant. Basani is not impressed and promptly informs Amu that she is not interested in pursuing a non-academic relationship with him. Amu is disappointed but is convinced that he can persuade her otherwise if he perseveres. He continues to message her in the chat and posts "romantic" material on her social media platform. He persists with this behaviour for months and escalates it to sending her inappropriate emails on a regular basis. He is not deterred by requests from Basani to stop the behaviour and does not respond to threats of pending police involvement.

At this point, subject to the definition of what constitutes stalking, these actions by Amu have to be considered to fall under the umbrella of Type II cybercrimes. According to the Gordon & Ford Categorisation (G&FC), from the perspective of the victim (Basani) these actions are not isolated events and do not involve the use of crimeware. It is here that the significance of labelling crimeware correctly becomes important, as the tools that have been used by Amu in this scenario are ordinary and neutral tools, in that they were not created with the aim of committing cybercrimes but merely as a means of communicating over the internet.

Assume, however, that the interactions between Amu and Basani do not end there. Amu has above average capabilities in the field of information technology and manages to acquire malware from the dark net. The purpose of this malware is to allow Amu to gain remote access to the Basani's webcam without her knowledge. He introduces this malware into her system by sending her a spam email that requires her to click a link provided therein. Basani is unaware that this is a spam email and her clicking the link downloads malware into her system, with her being none the wiser. Amu uses the malware to activate Basani's webcam and take pictures of her in her bedroom while she is getting dressed. He

then threatens to post these compromising pictures on her social media platform and distribute them to her colleagues at work unless she agrees to go on a date with him.

The introduction of malware presents a second dimension to the interaction between Amu and Basani. Essentially, the crime that is being perpetrated against Basani still falls within the ambit of Type II cybercrimes because it is largely still cyberstalking, blackmail and online harassment. However, the introduction of the malware provides a Type I cybercrime dimension because, firstly, it is a singular and isolated event from Basani's perspective (albeit within the context of prolonged harassment) and, secondly, it involves the use of crimeware. If legislators were to adopt this classification of cybercrime, they likely would have to devise a sentencing regime which caters for scenarios where there are overlaps. In other words, if legislative sanctions provide for a five-year prison sentence for Type I crimes and a 10-year prison sentence for Type II crimes, Amu would be found guilty overall of committing Type II cybercrimes with additional consideration for the one Type I cybercrime involving the crimeware.

Cybercrimes should be considered in terms of a continuum ranging from those crimes which are almost entirely technological in nature to those crimes which are in essence people-related. Gordon & Ford construct the table below to illustrate the point. This table classifies the different cybercrimes as either Type I or Type II and then records the software that is used in each case.

Table 1: Cybercrimes by Type[39]

Example	Type	Software	Crimeware
Phishing	I	Mail Client	No
Identity Theft	I	Keylogger, Trojan	Yes
Cyberstalking	II	email Client, Messenger client	No
DDoS	I	Bots	Yes
Cyberterrorism (communication)	II	Steganography, Encryption, Chat Software	No

39 Gordon & Ford (2006) at 16.

It is rare that one will find a cybercrime that is purely Type I or purely Type II, as attackers readily deploy whichever means will achieve the desired and best result. Accepting that cybercrime exists on a continuum will enable us to recognise the scale on which it exists and also to identify the areas in which different parties fall short. For example, police investigators are more likely to be able to handle people-centric cybercrimes whereas cybersecurity practitioners would be inclined to focus their efforts on technologically based crimes.[40] Recognition of this distinction allows for enhanced co-operation and would yield improved results.

2.4 The Gordon & Ford Categorisation and the Cybercrimes Act

The G&FC has been adopted in this study because it is helpful in evaluating the offences which are contained in the Cybercrimes Act. The conceptual framework allows us to classify the offences into Type I or Type II cybercrimes by asking two questions:

1. Is the act a singular or isolated event?
2. Is the act facilitated by crimeware?[41]

If the answer to both these questions is yes, then the offence concerned most likely is classifiable as a Type I cybercrime; and if the answer is no to both questions, it is most likely a Type II cybercrime.

The Cybercrimes Act provides for both Type I and Type II cybercrimes. Chapter 2, Part I of the Act, titled "Cybercrimes", identifies nine such offences. Type I offences span sections 2 to 10. They are:

- unlawful access;[42]
- unlawful interception of data;[43]
- unlawful acts in respect of software or hardware tool;[44]
- unlawful interference with data or computer programme;[45]

40 Gordon & Ford (2006) at 16.
41 Gordon & Ford (2006) at 14 include a third consideration which accepts that the crimeware sometimes can be introduced into the computer through a vulnerability. However, it is not necessary to add a third question because this element can fit neatly into the considerations regarding crimeware.
42 Section 2 of the Cybercrimes Act.
43 Section 3 of the Cybercrimes Act.
44 Section 4 of the Cybercrimes Act.
45 Section 5 of the Cybercrimes Act.

- unlawful interference with computer data storage medium or computer system;[46]
- unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices;[47]
- cyberfraud;[48]
- cyber forgery and uttering;[49] and
- cyber extortion.[50]

Although the offence of cyberfraud in section 8 of the Act is classified as a cybercrime, it is submitted that this classification is incorrect. The offence of cyberfraud is not a true cybercrime because it is only computer enabled not computer dependent, and it is not an attack on the confidentiality, integrity and availability (CIA) triad. The concept of a computer enabled crime is defined as "the use of data, a computer device, a computer network, a database or an electronic communications network to commit a prohibited act".[51] This distinction will be unpacked later.

The Type I and Type II categorisation of cybercrimes provides a clear method for differentiating between the two variants. Type II cybercrimes, such as cyberfraud, non-consensual pornography over the internet and cyberbullying, have been accepted widely as deserving of legislative intervention primarily because of the harm they occasion. In this study, the categorisation is accepted but the conclusion that Type II offences are true cybercrimes is not. It is submitted that while Type II cybercrimes have a significant presence in cyberspace, they do not meet certain minimum requirements which would warrant their elevation from ordinary terrestrial crimes to cybercrimes proper. It will be argued in the next chapter that they should not have been included in the Cybercrimes Act. Instead, the common law and the legislation which caters for them currently should be amended to encompass their presence in cyberspace and the harm they cause.

46 Section 6 of the Cybercrimes Act.
47 Section 7 of the Cybercrimes Act.
48 Section 8 of the Cybercrimes Act.
49 Section 9 of the Cybercrimes Act.
50 Section 10 of the Cybercrimes Act.
51 Section 2(1) of the Cybercrime Act.

2.5 Routine Activities Theory

Cybercrime is a complex and relatively new threat when compared to terrestrial crime. The aim of this study is to understand cybercrime as a form of criminality in its own right. This means that, in order to tackle cybercrime successfully, it is important to determine where it fits into the criminal law and to do so in a way that does not comprehend its various forms simply as analogies of conventional crimes. While there may be a number of common characteristics between ordinary crimes and cybercrimes — such as unlawful access to data or property — certain cybercrimes, by their nature, do not have "real world" counterparts amongst the conventional crimes. Furthermore, some cybercrimes encompass multiple factors and stages which may require different levels of legal responses.

Consider for a moment the earlier example of the phishing attack on Cassandra. It is, for all intents and purposes, a Type I attack but has many different elements that may be dealt with in different ways, with each element, as a crime, carrying an individual sentence upon conviction. The hypothetical of the phishing attack seeks to show that a superficial understanding of the basics of cybercrime has the potential to render the criminal law ineffective in the face of a single but multifaceted attack. There thus is a need to examine the place of cybercrime in the landscape of the criminal law and, to this end, the study will employ the precepts of Routine Activities Theory, as explicated below. Routine Activities Theory (RAT) was formulated by Cohen & Felson and it has become one of the most widely cited and influential approaches in criminology.[52] The compositional framework of RAT was elaborated in relation to the post-World War II period in the United States, when crime trends were observed to be related to patterns called routine activities. Routine activities are defined as:

> any recurrent and prevalent activities which provide for basic population and individual needs, whatever their biological or cultural origins.[53]

In the original formulation of RAT, the routine activities that were considered included formalised work, the provision of shelter, standard food, sexual outlets, childbearing and social interactions.[54] Cohen & Felson note that routine activities can go beyond the

52 Miró (2014) at 1; See also Leukfeldt & Yar (2016); Reyns (2017); Holt, Leukfeldt & van de Weijer (2020); Kigerl (2021).
53 Cohen & Felson (1979) at 593.
54 Cohen & Felson (1979) at 593.

minimum requirements for the continuity of the human species; all that is required is that the prevalence and recurrence of these activities be a part of everyday life.[55]

RAT has been developed and fused since with other approaches to crime analysis. However, it still rests upon the three factors which are essential for the commission of a predatory crime. The first is a supply of motivated offenders, the second is the availability of suitable targets or opportunities to commit the crime, and the third is the absence of capable guardians. It is emphasised that the lack of any of these elements is sufficient to prevent the perpetration of the offence.[56]

The theory specifies the kind of criminal violations with which it is concerned, namely, direct-contact predatory violations. Predatory violations are defined as "illegal acts in which someone definitely and intentionally takes or damages the person or the property of another".[57] Furthermore, the theory is confined to offences that involve direct physical contact between offender and target.[58] It should be noted that target, as opposed to victim, was chosen purposefully with a view to capturing also scenarios where a human is not directly and physically harmed by the offence. For example, a burglar could break into a home and steal objects while the occupiers are away. In this instance, the objects stolen cannot be referred to as victims but rather are targets. This distinction is vital because the word "target" is meant to highlight the fact that the theory focuses on offending from the viewpoint of the offender rather than that of the victim or society.[59] An example of a situation where a target could be referred to also as a victim would be a sexual assault or, to take a cyberspace example, cyberbullying in which victim and target converge.

One of the attractive features of RAT is that its approach can be contrasted to other theories of crime which are focused on the criminal himself, that is, on the psychological, biological or social factors that motivate or drive him to offend.[60] RAT takes it as a given that individuals have criminal inclinations and, therefore, examines the social structures that allow people to commit offences.[61] To focus on the offender's viewpoint, as noted above,

55 Cohen & Felson (1979) at 593.
56 Cohen & Felson (1979) at 590.
57 Glaser (1971) at 4.
58 Cohen & Felson (1980) at 390.
59 Felson (2008) at 71.
60 Miró (2014) at 1.
61 Cohen & Felson (1980) at 390.

means to focus on why he regarded the target as suitable, rather than on what motivated him to take or harm the target.

2.5.1 Spatio-Temporal Character of RAT

Routine Activities Theory studies criminal violations as events which occur at specific locations in space and in time and which involve specific persons and/or objects.[62] As intimated above, the aetiological formula of RAT is:

crime = motivated offender + suitable target – capable guardian

In order to explain this formula and/or anticipate trends in offending, the three constitutive elements need to converge in space and time. At the micro level, this means that, in order for a crime to be committed, both the offender and the target need to be present at a particular location at the same time, and the guardian needs to be absent.[63] At the macro level, the theory posits that there are a number of features in the larger society and larger community which can make the convergence of these essential elements more likely.[64] Routine activities are what create the variable environment where such spatial and temporal convergence can occur to provide suitable targets for offenders. According to Cohen & Felson, the organisation of time and space is central to RAT as it helps to explain how crime occurs and what needs to be done about it.[65]

For RAT to be applied to the virtual environment, cyberspace needs to exhibit spatio-temporal characteristics that are compatible with those of the "physical world". Place, time, proximity and distance need to be identifiable features of cyberspace.[66] In point of fact, the language of cyberspace is inundated with references to space and place, such as "portals", "chatrooms", "sites" and "backdoors", which are all linked to information "superhighways" with "ports" connecting some parts of the internet to other parts.[67] There are differing opinions as to whether these terms are merely handy metaphors adopted to help make sense of an anti-spatial and non-linear environment, or whether they denote actual spatial

62 Cohen & Felson (1980) at 390.
63 Yar (2005) at 414.
64 Felson (2008) at 70.
65 Cohen & Felson (1980) at 147.
66 Yar (2005a) at 414.
67 Adams (1998) at 88-89.

qualities.[68] Cyberspace is perceived to be an environment which is always only one click away, because of how thoroughly interconnected it is; conventional barriers of geography and national borders are not as present in cyberspace as in the terrestrial world.[69] This circumstance may suggest that the design of the internet is not compatible with the central requirements of space and time. However, cyberspace does possess certain redeeming characteristics.

Yar submits that those who hold the position that there is no recognisable spatial topology in cyberspace draw their conclusion from the belief that there can be an absolute separation of the virtual environment from the non-virtual environment.[70] Those who hold opposing positions suggest that the cyber environment should be conceived as a "real virtuality" rather than a "virtual reality". They view cyberspace as an extension of the terrestrial world where political, economic, social and cultural relations are conducted.[71] This is not to say that the two environments are the same and should be treated in the same way, but rather that there is no unbridgeable dichotomy between them.

While chatrooms and portals exist in the virtual space, the internet itself is physically rooted in the "real world" and produced in real space.[72] For example, as of 2021, forty per cent of all websites have their servers located in the United States,[73] with Asia having the largest percentage of internet users in the world at fifty five per cent.[74] The same inclusionary and exclusionary criteria, such as wealth, education, gender and ethnicity, which exist in the real world, structure access to cyberspace and usage of the internet. In other words, the capacity distribution of the internet reflects the social and economic hierarchies that exist in the real world. Thus, even though the internet is non-linear, it is profoundly spatialised. In short, the distribution of potential offenders and potential targets is not neutral, but dependent upon the distribution of cyber resources and skills.[75] Russia, for example, has highly skilled hackers and they are responsible for a great majority of the

68 Yar (2005a) at 415.
69 Dodge & Kitchin (2001) at 62.
70 Yar (2005a) at 416.
71 Castells (2002) at 203.
72 Yar (2005a) at 416.
73 W3Tech (2021) at 1.
74 Internet World Stats (2021) at 1.
75 Yar (2005a) at 416.

world's spam.[76] Also, suitable targets are more likely to be found in the United States than in South Africa because of the ubiquity of the internet and internet usage in the former.

2.5.2 Motivated Offender

The first essential element of Routine Activities Theory is the presence of a motivated offender. A potential offender may be anyone who has the motive to commit an offence and the capacity to do so. Felson (among others),[77] in his later work on RAT, avoided using the term "motivated offender" because he considered it to be important to focus not on the disposition or the inclination of the offender but on the physical factors that made it possible for a person to become involved in the commission of an offence.[78] Focusing on the physical features does not mean necessarily that the perspective of the offender is dispensable, as the determination of what makes a target suitable is dependent on the offender's purposes and capacities in relation to the intrinsic characteristics of the target.[79]

2.5.3 Suitable Target

The original aim of the theory that routine activities could explain crime trends was tested to confirm four hypotheses. The first was that the spreading of activities away from the home contributed to greater opportunities for offenders to gain access to suitable targets. The second was that the suitability of targets influenced predatory contacts. The third was that the victimisation rates could be increased by solitary life away from home. The fourth was that the structure of daily life was related to the rise in crime.[80] For purposes of the analysis of cybercrime, the second hypothesis pertaining to a suitable target is most relevant as it is one of the three core elements of RAT.

Target suitability consists of four constituent properties, namely, value, inertia, visibility and access, rendered by the acronym VIVA. In brief:

- The value of targets influences their desirability to offenders.

76 Krebs (2014).
77 Felson & Boba (2010) and Cohen & Felson (1980).
78 Miró (2014) at 2.
79 Miró (2014) at 2.
80 Miró (2014) at 2.

- Inertia refers to the mobility of the target, as determined by how big or heavy the target is, or whether it is attached to a lock, or whether the targets for personal violations may be able to resist.
- A target's visibility concerns the significant risk factor for being identified by the offenders.
- Finally, accessibility encompasses the location of the target and how suitable it is for the offender to gain legal or illegal access to it for purposes of committing a violation, as well as the opportunities available for non-detection and escape.[81]

The constituent properties of target suitability, as expressed in VIVA, are discussed individually and in more detail below.

2.5.3.1 Value

The value of a suitable target will vary depending on how it is viewed socially and economically at a particular juncture. Value can be monetary or symbolic, for use or resale, and would include any prejudice, challenge or sexual gratification that the offender might obtain from the target or the victim.[82] Currently, most of the suitable targets for cybercrime take the form of information and digital code.

Property, for example, comes in the form of intellectual property, movies, music, trade secrets, computer software and so on. Property of this nature has become increasingly more valuable to motivated offenders as potential targets for theft.[83] The range of targets may be extended in cases where the motivated offenders pursue suitable targets for trespass and criminal damage. The cybercrime case in point is "hacking", which would encompass the invasion of computer systems and websites, the distribution of malware and the damage caused by viruses and worms.[84] Additionally, individuals could be targeted for stalking or bullying, or because they are members of a particular religious, ethnic, racial or social group. As RAT examines criminal offences from the perspective of the motivated offender, the value of targets will depend on what the offender perceives as valuable.

81 Cohen & Felson (1980) at 393.
82 Yar (2005a) at 419.
83 Yar (2005a) at 419.
84 Clough & Mungo (1992) at 85-105.

Broadly speaking, it may be concluded that, when it comes to determining the suitability of targets to the motivated offender, the valuation process varies as much in cyberspace as it does terrestrially.[85]

2.5.3.2 Inertia

As intimated above, inertia refers to the physical properties of the target. There is an inverse relationship between the suitability of the target and inertia, in that the suitability of the target decreases as the inertial resistance increases, and vice versa.[86] At first glance, this relationship between inertia and suitability would appear not to apply to virtual property because the targets of cybercrime, being digitised, seem weightless. Technological advances have allowed information to be downloaded and replicated seemingly instantaneously, with the obvious example being pirated information or property in the form of movies and music. However, closer inspection of the properties of the virtual environment indicates that the goods in cyberspace do retain some inertial characteristics.[87]

Firstly, the volume of data can provide great resistance to suitability, particularly in situations where the internet connection is not sufficiently potent to commit the offence. Secondly, it is necessary that the motivated offender have appropriate tools to carry out his criminal plans. For instance, in order for an offender to be able to steal a significant amount of data, he will need sufficient storage, in the form of hard drive space, in which to deposit that data. Therefore, although virtual information may have relatively less inertial resistance as compared to terrestrial property, its weightlessness is not absolute.[88]

2.5.3.3 Visibility

RAT postulates that visibility, unlike inertia, has a positive correlation with suitability in that an offender must know that a target exists in order to offend.[89] Persons who are and property that is prominently visible are more likely to be targets. This relationship is somewhat more obvious terrestrially than in cyberspace where it may seem more difficult

85 Yar (2005a) at 419; Leukfeldt & Yar (2016) at 269.
86 Yar (2005a) at 420; Leukfeldt & Yar (2016) at 270.
87 Leukfeldt & Yar (2016) at 265.
88 Yar (2005a) at 420.
89 Bennett (1991) at 148; Leukfeldt & Yar (2016) at 270..

to conceptualise the visibility of a target. However, there is no lack of target visibility in the realm of cyberspace.

In the absence of tools such as closed ICT networks (for example, intranets and virtual private networks) which are designed to reduce access or hide the virtual presence of a user, the internet is inherently public. The internet is designed not to be limited by barriers of physical distance. This means that, in essence, virtually present objects are globally visible and therefore suitable targets. This global visibility may operate to advertise the existence of the targets to the largest pool of offenders.[90] The popularity and interconnectedness of social media and social networks, for example, mean that more people are exposed more and can be targeted easily for cyberstalking and cyberbullying.

2.5.3.4 Accessibility

Accessibility also has a positive correlation with suitability. The easier it is to access the target and get away from the scene of the crime, the greater the suitability of the target. For terrestrial crimes, a house that is situated in a *cul-de-sac* generally is less accessible and less desirable than a corner house because the possibilities for escape without detection from a *cul-de-sac* are limited.[91] Accessibility is one of the attractive traits of cybercrime because traversing cyberspace is "non-linear". This means that it is possible to jump from one place to another in a matter of moments and disappearing from the "scene of the crime" can be as easy as severing the connection with the network.[92] It is still possible, though, that the cyber offender may be detected by security features (for example, by an Intrusion Detection System) in the target network during the commission of the crime and subsequently traced back to his "home" network. However, there are many tools readily available to circumvent attempts to trace the offenders, including anonymous remailers, encryption devices, and the use of third party servers and systems.[93]

90 Yar (2005a) at 421.
91 Beavon et al. (1994).
92 Newman and Clark (2003) at 17 63.
93 Grabovsky and Smith (2001) at 35.

2.5.4 Capable Guardian

The third pillar of RAT is that an offence can be successful only in the absence of a capable guardian. Cohen & Felson describe a capable guardian as including traditional law enforcers, such as police officers and security guards, but maintain that the concept should not be limited to such enforcers.[94] This approach is beneficial to an examination of cybercrime because it provides for possible alternative types of guardians in relation to deal the complexities of cyber offences. Cybercrime forces us to think about crime differently and, by the same token, preventing cybercrime should be conceptualised differently since traditional law enforcement strategies will not attain the same level of effectiveness in the cyber world as in the terrestrial one.

A capable guardian plays a critical role in crime and its prevention as he is someone who intervenes in the designs of the offender, however inadvertently.[95] A capable guardian is anyone in whose presence a crime will not be committed and in whose absence the crime likely will be committed.[96] In this definition, the notion of a capable guardian is not limited to a security guard or a police officer but refers to anyone who moves through an area acting as a protector of property or persons, even a bystander.[97] The capable guardian may be cast in three roles, as a guardian, a handler or a manager.

A capable guardian can deter crime in the context of social control, as in a relationship with the offender (as handler), a relationship with the place (as manager) or a relationship with the target itself (as guardian). Handlers have an emotional relationship with the offender, which can range from family or friendship ties, to religious or other similar connections. The objective of the handler is to ensure that the offender avoids problematic situations. Managers are the owners or the agents of the place, such as doormen, waiters, store employees and the like. Finally, guardians seek to protect the target

94 Felson (1980) at 53.
95 Felson (1995) at 53.
96 Felson (1995) at 53.
97 Miró (2014) at 3; Leukfeldt & Yar (2016) at 270.

itself. These are not merely police and security guards but, by and large, are the owners of the property that they guard.[98]

An interesting aspect of the capable guardian model is that it does not place too much store by formal police and security guards. The reason lies in the fundamental assumption underlying the theory, that the most important aspect of the guardian is availability and monitoring. The idea that needs to be given to the motivated offender is that there is someone who is keeping an eye on the target. The difficulty with formal law enforcers is that they are not available to watch over the target at all times, and are unlikely to be present when the crime occurs.[99]

This is an important consideration in the context of cybercrime, because the police hardly can be present where the cyber offences occur, especially given the vast space that the internet occupies. It becomes necessary, therefore, to consider new or improved ways of thinking about cybercrime prevention and law enforcement. This is not to say that police have no role in combating cybercrime, but rather that they need to adapt to the changing landscape of contemporary criminality. Cohen & Felson's capable guardian model provides a framework within which to consider alternatives. This aspect of Routine Activities Theory will be employed to study Chapter 6 of the Cybercrimes Act and to assess whether it will be effective in combating cybercrime.

98 Miró (2014) at 4.
99 Felson & Boba (2010) at 28.

CHAPTER THREE

TYPE I CYBECRIMES: THE MOTIVATED OFFENDER

3.1 Introduction

This chapter discusses the offences contained in Part I and Part II of Chapter 2 of the Cybercrimes Act. The discussion is informed by the philosophical precepts of this study, in particular the motivated offender as described by Cohen & Felson's Routine Activities Theory and Type I cybercrimes as described by the G&FC. The offences identified in sections 2 and 3 of the Cybercrimes Act are referred to collectively as hacking offences.

The chapter begins with a discussion of the definition of cybercrime. It proposes the adoption of the CIA triad and classification as computer-dependent as minimum requirements for defining cybercrime and for differentiating Type I from Type II cybercrimes. It then proceeds to discuss the individual offences contained in the Cybercrimes Act, paying particular attention to Type I cybercrimes.

3.2 Definitional Considerations

The United Nations Office on Drugs and Crime (UNODC), in a comprehensive study, states that the definition of cybercrime depends on how the term is used.[1] Acts which violate the confidentiality, integrity and availability (the CIA triad) of computer systems are regarded as being at the core of cybercrime. Therefore, other acts, such as those where the target is the victim herself or acts committed for personal or financial gain or harm, will fall within the wider meaning of cybercrime.[2] Examples of these include identity-related acts, certain fraudulent acts, cyber sexploitation and other mainly Type II cybercrimes. The UNODC study records that some of these acts or crimes do not lend themselves to arriving easily at a legal definition of the aggregate terms of cybercrime. It is interesting that such a comprehensive study has not attempted to identify a viable definition of cybercrime (dispensing with the question in a single paragraph), thereby perhaps suggesting that it may not be a worthwhile

1 UNODC Study (2013) at xvii.
2 UNODC Study (2013) at xvii.

exercise in which to engage. Alternatively, the UNODC's approach could be an indication of the incredible difficulty of defining the concept.

As was noted previously the Budapest Convention also does not provide a definition of cybercrime, nor does the Cybercrimes Act,[3] which has opted to follow the approach taken by the Budapest Convention of describing acts which constitute cybercrimes. However, skirting the exercise of defining cybercrime is not common practice, as many guides, reports and publications begin with a definition and where they are unable to provide a comprehensive definition, at least they admit so and explore the associated difficulties.

The International Telecommunication Union (ITU) issued a draft cybercrime legislation guide for developing countries,[4] highlighting some of the approaches to and difficulties of defining cybercrime. A common procedure is to describe cybercrime in terms of any activity that will have computers or computer networks as the target of the crime, the tool for committing the crime or the place where the crime is committed.[5] Another approach is to consider the objectives of the cybercrime in order to describe its constitution.[6] The ITU guide concludes by acknowledging that there is no one criterion that could be applied to encompass all the acts which have been identified in the Budapest Convention, for example. It also observes that the fact that there is no single definition of cybercrime should not be a problem for as long as the term is not used as a legal concept, because in civil law countries its use can lead to legal uncertainty.[7]

This latter point is an interesting one, prompting a follow-up question: does the absence of a settled definition of cybercrime bar domestic legislation and policy from creating a definition which would have at least the agreed upon essential elements of cybercrime? In other words, could South Africa decide upon its own definition for the purposes of the Cybercrimes Act, which definition includes the minimum requirements for criminalising any act which threatens the confidentiality, integrity and availability of a

3 The Explanatory Notes at 63 acknowledge that there is not a settled definition of cybercrime but suggests that a possible definition of cybercrimes could be "crimes which are committed by means of, or which were facilitated by or which involve data, a computer programme, a computer data storage medium or a computer system".

4 ITU Guide (2009) at 15.

5 ITU Guide (2009) at 15.

6 ITU Guide (2009) at 15.

7 ITU Guide (2009) at 15.

computer system? On the one hand, this would help clarify the legal position of each jurisdiction whilst allowing for internationally recognised minimum requirements. On the other hand, it could create further difficulties when it comes to jurisdictional concerns. Perhaps the national approach might not be desirable, considering that cybercrime does not respect national borders, making international co-operation imperative. Nevertheless, it is a point worth pondering.

Gordon & Ford think that it might be significantly beneficial to delete the term "cybercrime" from the lexicon entirely, although they recognise that that is unlikely to happen.[8] They opt instead to define a cybercrime as "any crime that is facilitated or committed using a computer, network, or hardware device".[9] This definition is very wide, hence their advocacy of a two-type categorisation of cybercrime. Furthermore, they contend that a computer or device may be the agent of a crime, the facilitator of a crime or the target of a crime, which is a position similar to the one taken by the ITU.

This study supports the approach taken by the UNODC, which limits the core cybercrimes to the ones that are committed against the CIA triad. The quest for concise and effective cybercrime legislation would benefit if the designated crimes are the ones that have a very close link to the CIA triad. This approach argues that it is imperative to have prescribed guidelines or set parameters in terms of which offences are captured under the umbrella of cybercrime in order to prevent, firstly, the criminalisation of conduct which does not meet the minimum requirements and, secondly, the creation of offences which would be more appropriate in a different piece of legislation. For the Cybercrimes Act to be effective, it needs to have a singular focus and not be diverted by cyber-adjacent offences which may render it ineffective.

The first step in prescribing guidelines is to differentiate between computer-dependent and computer enabled offences. This is of paramount importance because it determines whether a crime is a true cybercrime or not. The G&FC splits along these lines, where Type I crimes are computer dependent and Type II crimes are computer enabled. This chapter will focus on computer dependent crimes. Further, in keeping with RAT, it will

8 Gordon & Ford (2006) at 14.
9 Gordon & Ford (2006) at 14.

consider the first essential element for determining the social factors that allow for the successful commission of a crime, namely, the presence of a motivated offender.

Computer enabled offences will be discussed in Chapter Four, where it will be argued that they should not have been included in the Cybercrimes Act because they are not true cybercrimes. Given that Type II crimes are not limited by the CIA triad as the primary target, the second essential element of RAT — which is the presence of a suitable target — will be the focus of that discussion. The final element of RAT — the absence of a capable guardian — will be discussed in Chapter Six.

3.3 Computer-Dependent Crimes and the CIA Triad

Computer-dependent crimes are crimes that can be committed only by using a computer, computer networks or any other form of ICT. Some of the acts that are included in this form of crime are the spread of malware, hacking and denial of service attacks.[10] Computer-dependent crimes fall into two broad categories. The first is illicit intrusion into computer networks, as in the case of hacking offences. The second is where computer systems are disrupted or downgraded, as in the case of viruses and (distributed) denial of service (DDoS) attacks.[11] The primary aim of computer-dependent crimes is to attack and deplete network resources, but it is also common for there to be an assortment of secondary outcomes, for example, using stolen data to commit computer enabled offences such as fraud.[12] The Type I crimes considered in this chapter are discussed in terms of their primary aim of attacking and depleting network resources.

At this juncture it is necessary to describe some of the technical weapons that enable Type I crimes to be committed in order thereby to gain a better understanding of the offences that are being legislated.

- *Malware* is a label that is used generally for describing malicious software which is spread across computer systems and interferes with computer operations. Malware can be destructive, as where it deletes files or causes computer systems to crash and

10 Sallavaci (2017) at 53.
11 McGuire & Dowling (2013) at 4, Wadhwa & Arora (2017) at 2218.
12 McGuire & Dowling (2013) at 4, Wadhwa & Arora (2017) at 2218.

operate at suboptimal levels. Malware comes in a variety of forms such as viruses, worms, Trojans and spyware.[13]

- *Viruses* are self-replicating programmes which spread within and between computer systems. They cannot run or be activated without a human executing a command, such as opening an infected file. It can be spread by the sharing of computer files from on user to another.[14]
- *Worms* do not need a human to execute a command. They are also self-replicating but, unlike viruses, can operate autonomously, without requiring a host (such as a file, disk or spreadsheet) to act as a carrier. Worms, therefore, can have more deleterious effects than viruses. Worms can be used to drop Trojans onto a network system.[15]
- *Trojans* are forms of malware which wear the guise of legitimate software or programmes but actually facilitate illegal access to a computer. Unlike other viruses, it will neither multiply nor infect other files on purpose, rather it would induce a user to download it so as to give the attacker a channel to the target's computer.[16] Some of the functions that a Trojan can perform include clandestinely stealing data and tricking users into believing that it is executing a routine task whereas, in reality, it is performing a hidden and unauthorised task.
- *Spyware* is a type of malware which invades a user's privacy by gathering sensitive or personal data from infected systems. It can do this also by monitoring the websites which are visited by the victim. This information then may be transmitted (sold) to third parties.[17]
- *Hacking* is a form of trespassing on a computer system.[18] It can present in a variety of ways and for a variety of reasons. It is used typically as a one-size-fits-all term that encompasses various types of unauthorised access to a computer system.

13 Wadhwa & Arora (2017) at 2218.
14 Shahrear et al (2017) at 12.
15 Mondal et al (2020) at 363.
16 Zhang (2018) at 1017.
17 McGuire & Dowling (2013) at 5.
18 McGuire & Dowling (2013) at 5.

- A *DDoS* attack is an attack where internet servers are flooded with so many requests that they are unable to respond quickly enough, leading to the servers being overloaded and subsequently crashing.[19]
- *Botnets* are clusters of malware-infected computers. They often are referred to as "zombie" computers because they are controlled centrally by a "botmaster" repeatedly and continuously to send out spam emails and carry out DDoS attacks.[20]
- *Spam* is unsolicited or "junk" emails which are sent out in bulk to countless and random recipients. Oftentimes the emails are used for marketing purposes. Spam is used heavily in the pharmaceutical and pornography industries, and for phishing and distributing malware.
- *Phishing* is defined broadly as "the creation and use by criminals of emails … in an attempt to gather personal, financial and sensitive information".[21] A phishing attack typically is carried out via an email service, although there are instances where it can be done via SMS (*SMiShing*) and via voice phishing (*vishing*) with the use of Voice over Internet Protocol (VoIP) technology.[22] Phishing attacks can range from being relatively simple to being quite sophisticated, for example, lacing emails with malware that can infect the victim's computer with key logging software or Trojans. Such malware can collect information about the target without her knowledge and, in the event that the victim responds positively to the fraud, she may be added to a "suckers list" which may be circulated amongst the criminals, leading to repeated re-victimisation.[23]
- *Spear phishing* refers to a phishing attack that is targeted at a specific person or group of people.[24]

19 McGuire & Dowling (2013) at 5.
20 McGuire & Dowling (2013) at 6; See Antonakakis et al (2017) for a discussion on the Mirai botnet attack of 2016.
21 Binational Working Group (2006) at 4. The word "phishing" is a variant of the word "phreaking", which was a term used in the early days of hacking, where a hacker would manipulate telephone systems to be able to make unauthorised long distance calls.
22 Clough (2015) at 223.
23 Cross *et al* (2014) at 3; National Fraud Authority (2008) at 44.
24 Binational Working Group (2006) at 8-9.

The various tools and transgressions listed above are at the core of Type I cybercrimes. While each of these may constitute an attack on its own, in many cases they overlap: for example, in order to execute a DDoS attack, one needs to use a botnet. Typically, computer-dependent crimes focus on personal profit or financial gain, as in cases of hactivism or the use of malware to steal confidential information. These motivations may be determined from the programmes or tools that are used in the commission of the crime. For example, spam containing phishing malware clearly is aimed at financial gain by targeting bank account information.[25]

The CIA triad is central to the determination of whether an act is a cybercrime or not. It is also the first indicator of whether an offence is computer-dependent or computer enabled. The CIA triad is one of the fundamental tenets of information security, encompassing, as intimated above, the protection of confidentiality, integrity and availability. The term was coined in 1986 by Ross A Leo.[26] Since its inception, the CIA triad has been the *de facto* standard against which organisational security policies have been designed. The triad is used to identify problem areas and produce solutions to those problems.[27] The National Institute of Standards and Technology (NIST) defines the terms of the triad in the following manner:

- *Confidentiality* refers to preserving authorised restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.
- *Integrity* entails guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- *Availability* seeks to ensure timely and reliable access to and use of information.[28]

The way in which information security has developed since the inception of the CIA triad has changed phenomenally, and cybercrime and cybersecurity concern far more than information security. The way in which information is transmitted, secured and stored has changed also. The threats to information no longer are limited to technical difficulties but

25 McGuire & Dowling (2013) at 6.
26 Chief of Technical Operations and Assurance for Data Trust Company.
27 Pender-Bey (2012) at 5.
28 NIST Special Publication 800-37-rev 1, Appendix B Glossary.

encompass a vast collection of events that include accidental loss, destruction, theft, modification (intended and unintended), natural and environmental elements and the all-important human element.[29]

In 2002, Donn B Parker presented an expanded model of the CIA triad as he believed that the original was insufficient to encapsulate all the developments in information security. In his view, it was too simplistic, in the sense that it could not account for the fact that security is also about people, not just about technology. He argued that the CIA triad focused too much on the technology and not enough on the people. He refers to the original CIA triad as the current information security model while styling his own expanded version the new information security model.[30] This model later was renamed the Parkerian Hexad in honour of Parker.

The Parkerian Hexad expresses a set of components added to the CIA triad to present a complete and comprehensive new model of information security. The constituent six atomic elements of the Parkerian Hexad are confidentiality, integrity, availability, authenticity, possession or control, and utility. The new elements were added not to replace the CIA triad but rather to expand it in a way that makes it more comprehensive. Parker thought it best that these elements were understood and implemented when they are grouped in the following manner: confidentiality and possession; integrity and authenticity; and availability and utility.[31] Each of these groupings will be discussed in turn below.

3.3.1 Confidentiality and Possession

Possession is the element that Parker appended to confidentiality. It was created to protect against the idea that a person can lose possession or control of information or data without necessarily breaking confidentiality. It seeks to make the point that retaining possession is vital when one is trying to maintain confidentiality. In a sense, it provides a second level of protection of data.[32]

Take, for example, cases where a security engineer's laptop containing sensitive information is stolen while she is working from home. At this point, there has not been a

29 Pender-Bey (2012) at 5.
30 Parker (2010) at 13.
31 Pender-Bey (2012) at 12; Pender-Bey (2019) at 6.
32 Pender-Bey (2012) at 10; Pender-Bey (2019) at 6.

breach in confidentiality in that the thief has not gained access yet to the data because of the password on the laptop. However, it is foreseeable, from the engineer's perspective, that the loss of possession well may result in the confidentiality of the information being compromised.

The original CIA triad would consider only the security of the information and say that it is necessary to encrypt the data or have it password protected, but the expanded version recognises that it is necessary to guard against the loss of possession.

3.3.2 Integrity and Authenticity

Integrity is an original element of the CIA triad. Its aim in information security is to guard against the modification or destruction of information, regardless of whether this modification or destruction is done by a person who is authorised to have access to the information or not. This element includes ensuring that the information is protected from non-repudiation and is authentic.[33] It is common knowledge that, in organisations, it is the employees who are usually the biggest threats to the integrity of information because they may delete files unintentionally or accidentally, enter incorrect data, or save over an incorrect file. Furthermore, files can become corrupted through transferral from one point to another or through viruses.[34]

Authenticity is an addition by Parker to the CIA triad. Authenticity assures that the data being transferred comes from the source or the person from whom it claims to come.[35] For example, when one receives an email asking one to click on a link, authenticity assures one that it comes from the person, entity or source that one believes it to be. If a hacker sends a virus attached to a pdf document, that virus most likely maintains its integrity as the hacker would intend, and is not modified through the transferral from him to his victim. This means, in terms of the CIA triad, that the information is secure. However, it is not authentic because the victim believes that it is from a trusted party.

The possession element also helps in accounting for information or data that may not necessarily be confidential but still requires protection. Intellectual property — such as books, music and movies — are in the public domain but they are owned and may be

33 Parker (2010) at 14; Pender-Bey (2019) at 14.
34 Pender-Bey (2012) at 13.
35 Pender-Bey (2012) at 14.

copyrighted. Possession covers not only situations where confidentiality is vital but also situations where it is non-existent.

3.3.3 Availability and Utility

Availability is the last component of the CIA triad and it refers to the ability to have access to resources or data as and when needed.[36] Not only should data be available, it also should be useful. According to the CIA triad definition, in order for data to be defined as available, it merely needs to be usable but not necessarily useful. Parker differentiates between usable and useful data with this example: if one comes across encrypted data for which the decryption key is unknown, the data remains available (usable) for cryptanalysis but it is not useful in its present form. It is possible also to have data which is usable but not useful. Therefore, it is necessary to include a sixth independent state of utility which is defined as that which is useful or fit for some purpose.[37]

Parker is critical of the value of the CIA triad when it stands on its own because it may create a situation where information security is "an open-ended, faulty and imprecise art".[38] While Parker's critique may be valid, the CIA triad remains the foundation upon which anti-cybercrime legislation and regulations are built. Even the Parkerian Hexad itself does not do away with the CIA triad, it merely builds on it. For the sake of clear and effective legislation, the CIA triad remains essential. If for nothing else, it represents the minimum requirements for criminalising cyber misconduct.

3.4 Categorising Cybercrimes

Chapter Two above set out the philosophical basis of the study, namely, the Routine Activities Theory combined with the Gordon & Ford Categorisation. This section discusses the individual crimes contained in the Cybercrimes Act in terms of those philosophical tenets. In order to simplify the discussion, all the crimes that are related to one another will be grouped together and subcategorised as necessary. The reasons for grouping certain crimes will be given as each crime (or crime set) is discussed.

36 Pender-Bey (2019) at 15.
37 Parker (2010) at 17.
38 Parker (2010) at 17.

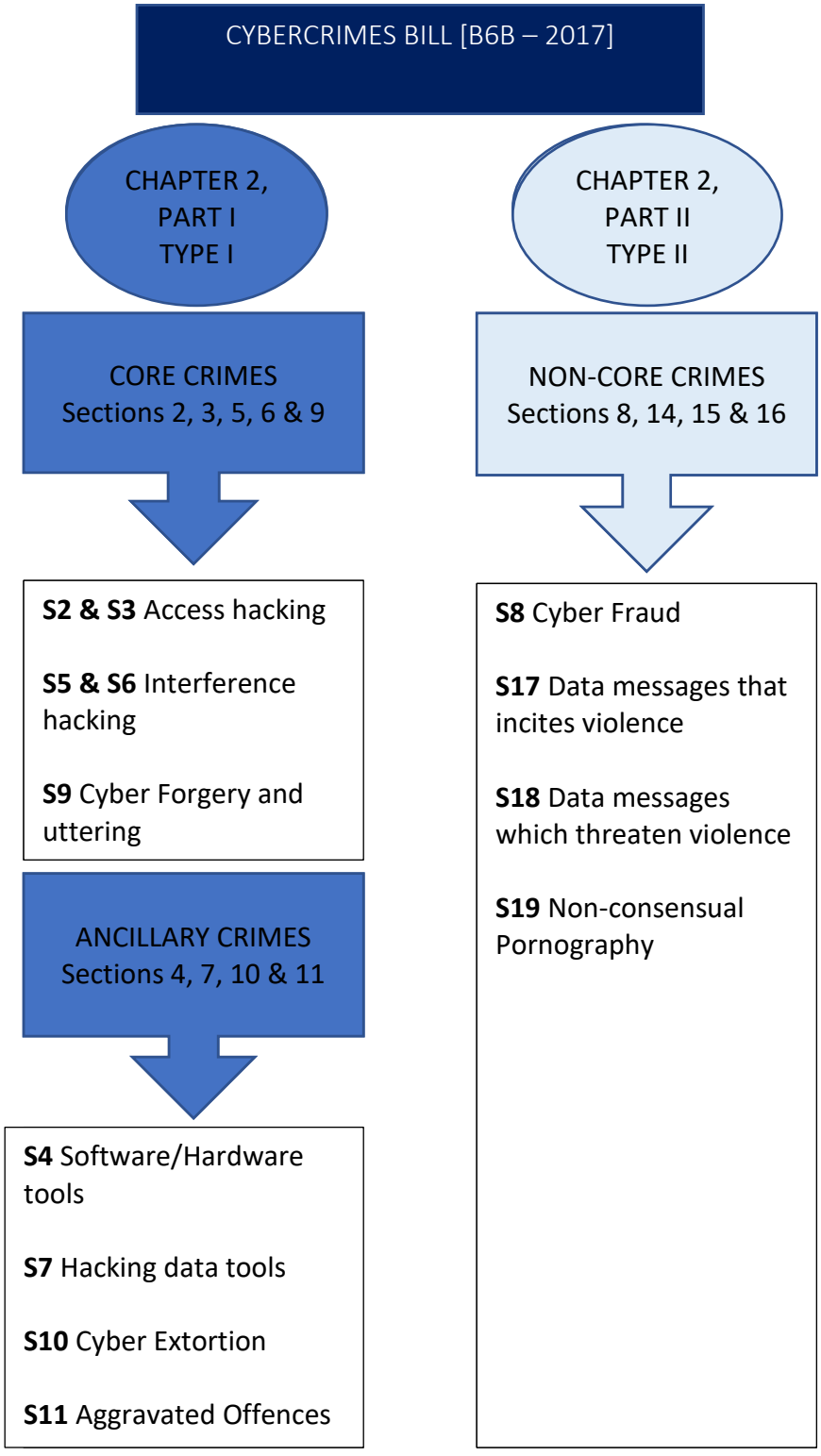
Part I of Chapter 2 of the Cybercrimes Act is titled “Cybercrimes” and it creates various offences. All these offences fit nicely under the banner of Type I cybercrimes. For the purposes of this study, sections 2, 3, 5, 6 and 9 have been grouped together and referred to as the core crimes of the Act, whereas sections 4, 7, 10 and 11 are referred to as the ancillary crimes. Each offence will be discussed in turn.

Below are two diagrams which show the categories. Diagram 2 is a simplified version of Diagram 1 which highlights further groupings.

Diagram 1: Core, Ancillary and Non-Core Crimes

CYBERCRIMES ACT 19 of 2020	
Chapter 2, Part I of Cybercrimes Act **Type I** **Computer dependent cybercrimes**	**Chapter 2, Part II of Cybercrimes Act** **Type II** **Computer enabled cybercrimes**
Sections 2, 3, 5, 6 & 9 **Core Crimes**	**Sections 8, 17, 18 & 19** **Non-Core Crimes**
Section 2 Unlawful access	**Section 8** Cyber Fraud
Section 3 Unlawful interception of data	**Section 14** Data message which incites damage to property or violence
Section 5 Unlawful interference with data or computer programme	**Section 15** Data message which threatens persons with damage to property or violence
Section 6 Unlawful interference with computer data storage medium or computer system	**Section 16** Distribution of data message of intimate image
Section 9 Cyber forgery and uttering	
Sections 4, 7, 10 & 11 **Ancillary Crimes**	
Section 4 Unlawful acts in respect of software or hardware tool	
Section 7 Unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or device	
Section 10 Cyber extortion	
Section 11 Aggravated offences	

Diagram 2 (Simplified Version of Diagram 1)



3.4 Unauthorised Access

As noted above, hacking offences feature prominently in the Cybercrimes Act. By way of introduction to hacking offences, consider the crime of illegal access in Article 2 of the Budapest Convention, which provides that parties should adopt legislative measures to criminalise unlawful and intentional conduct aimed at gaining access to the whole or any part of a computer system. It allows parties to require that the offence be committed by infringing security measures with the intent of obtaining computer data or any other dishonest intent.

Sections 2 and 3 of the Cybercrimes Act create the offences of unauthorised access to computer systems. Unauthorised access refers to conduct that directly threatens the integrity and the confidentiality of a computer system. It may not infringe necessarily on the availability of the computer system because, in most cases, the target still has her own means of access to it, even though the details in the system may have been compromised.[39] However, the infringement of the legal interests of the target does not occur only when there is an alteration in or theft of data from a computer system; merely "looking around" in the system would be sufficient to constitute an infringement.[40]

According to the explanatory report to the Budapest Convention, the offence of illegal access covers basic threats to and against the security of a computer system in relation to the CIA triad. It stipulates that the mere unauthorised intrusion into or access to a system — encompassing "hacking", "cracking" and "computer trespass" — should be illegal in principle. This is because such access or intrusion would deny legitimate users access to their own computer systems. Furthermore, it would compromise the security of the computer system because of the risk of confidential user information being revealed.[41] In this regard, authority is a key component in determining liability. If a technician or an employee has a right of access to a computer system but that right subsequently is revoked or limited, entry by said person into the computer system after the revocation or limitation would be unauthorised and, therefore, subject to criminal liability.

39 This may be contrasted with the offence of unlawful interference, contained in sections 5 and 6, which may infringe on availability directly.

40 UNODC (2013) at 82.

41 Budapest Convention, Explanatory Report (2001) at 11.

According to the Explanatory Report, the notion of "access" means entering the whole or a part of any computer system (incorporating hardware, components, stored data, directories, traffic and content related data). However, gaining access does not include the mere sending of an email or a file to the system. Also, "access" is not limited to entering a single or individual computer system but can apply also to gaining access via one system to another, through public communication networks, local area networks (LANs) or the intranet of an organisation. The method of communication, whether from a distance (including via a wireless link) or at a close range, does not matter.[42]

The intrusion must be committed "without right", meaning that there cannot be criminal liability for entering a computer system which permits free and open access by the public, such as access "with right".[43] There may be specific technical tools that could be used to gain access under Article 2 of the Budapest Convention, such as entry into a web page directly or through hypertext or deep-links; or entering through the application of "cookies" or "bots" which are used to retrieve information. The application of such tools *per se* is not "without right" because public websites needs them for purposes of maintenance and there typically is implied consent by the website owner granting access to any other web user. Furthermore, the application of standard tools in the commonly applied communication protocols and programmes is not itself "without right", particularly in cases where the right holder has not rejected their initial installation or removed them, as in the case of "cookies".[44]

Section 3 of the Cybercrimes Act prohibits the unlawful interception of data. Although the Budapest Convention does not make specific provision for the unlawful acquisition of data, presumably because of the close relationship between securing access and acquiring data, it does make provision for unlawful interference with a computer system.[45] This offence is contained also in sections 5 and 6 of the Cybercrimes Act. All in all, the offences referred to above collectively traverse the broad scope of criminal hacking.

The Explanatory Report to the Budapest Convention notes the different approaches which may be taken by states regarding the offences relating to hacking. Whereas the

42 Budapest Convention, Explanatory Report (2001) at 11.
43 Budapest Convention, Explanatory Report (2001) at 12.
44 Budapest Convention, Explanatory Report (2001) at 12.
45 Article 5 and Article 6.

Budapest Convention criminalises the mere intrusion into a computer system, some jurisdictions do not do so, because sometimes the intrusion may lead to the discovery of weaknesses in the security of the system.[46] This most likely would occur in cases of so-called grey hat hacking, which will be discussed later.

3.4.1 Elements of the Offence of Unauthorised Access

Section 2 of the Cybercrimes Act prohibits unlawful access to data, a computer programme, a computer data storage medium or a computer system.[47] For ease of reference, these will be referred to collectively as a "computer system" where necessary. The elements of this offence are: (a) unlawfulness, (b) intention, and (c) access to a computer system.

Section 2 provides that a person accesses a computer system when he or she is in a position to alter, delete or modify computer data or a computer programme; copy or move the data or programme to another storage medium (whether internal or external); cause the data or programme to perform any function; obtain its output; or otherwise use the data or programme.[48] The provisions pertaining to computer data and a computer programme apply to the data stored in a data storage medium or offences committed in terms of it.[49] They also provide for securing access to a computer system when a person is in a position to use any resources of, instruct, or communicate with the computer system.[50]

For purposes of this prohibition, the access must be accomplished with intention and it must be unauthorised. Unauthorised access represents the first element of the crime, namely, unlawfulness. According to section 2(3) of the Cybercrimes Act, unauthorised access can present in three ways. The first instance concerns a person securing access who is not lawfully entitled to do so.[51] This refers to a typical hacker scenario, where an offender can overcome the security measures in a computer system in order to secure access.

The second instance is a bit more nuanced. In essence, mere access can attract liability, even if the intention is not to attack or destroy the system. In this regard, it must be remembered that the element of intention is attached to the element of securing access

46 Budapest Convention, Explanatory Report (2001) at 12.
47 Section 2(1)(a)-(d) of the Cybercrimes Act.
48 Section 2(2)(a)-(b) of the Cybercrimes Act.
49 Section 2(2)(c) of the Cybercrimes Act.
50 Section 2(2)(d) of the Cybercrimes Act.
51 Section 2(1) of the Cybercrimes Act.

and not to the subsequent actions of the "offender". Consider section 2(2)(d), which provides that:

> for purposes of this section a person accesses a computer system when the person is in a position to use any resources of …[the] computer system.

Say, for instance, Basani leaves her work computer (which is not password protected) unattended when she goes to lunch and her colleague, Amu, decides he wants to check his emails on that computer. Amu might incur criminal liability under section 2(1) of the Cybercrimes Act. To use the language of the Act, by Amu checking his emails on Basani's computer, he accesses her computer system. Perhaps Amu could tender the (weak) counter-argument that, since the computer is a company computer, he has some kind of tacit right of access to it, and therefore there is no risk of unlawfulness.

However, even if that argument were to be tendered, the second instance of unauthorised access could apply, to the effect that access to a computer system is unauthorised when the person entering the system did not obtain consent from one who is lawfully entitled to have access.[52] This means that even if Amu argues that the computer system is company property, ultimately the one who is entitled lawfully to have access is Basani and, therefore, she would be the one permitted to give consent. Since she did not, Amu runs the risk of violating section 2 of the Cybercrimes Act.

The third instance in the meaning of unauthorised access arises when the offender initially is permitted access but the permission subsequently is revoked or the offender exceeds her authority. For example, Basani permits Amu to use her computer to check his emails and, after doing so, he uses her computer as a storage medium to transfer documents without her consent. Here Amu has exceeded the authority received from Basani and, theoretically, he may be held liable criminally.[53]

Although the probability of a person being held liable criminally for checking his emails on his colleague's computer seems unlikely, perhaps even absurd, the wording of section 2(2) of the Cybercrimes Act lends itself to a broad interpretation which indeed may lead to such absurdity. The objective of the section is easy to determine, and even though

52 Section 2(1) of the Cybercrimes Act.
53 Section 2(3) of the Cybercrimes Act.

the explanatory notes do not make it explicit, they do record that the criminalisation of unlawful securing of access represents an important deterrent for other acts which may assail the CIA triad.[54]

As noted above, the second and third elements of the offence of unauthorised securing of access are intention and securing access respectively. It was mentioned earlier also that the Explanatory Report to the Budapest Convention indicates that mere intrusion into or "merely looking around" in a computer system may be criminalised. The Cybercrimes Act appears to have adopted this position in section 2.

The wording of section 2 is somewhat peculiar in the way it speaks of securing access. It provides that a person accesses a computer system when said person is "in a position to" alter, delete, and modify data and the like. This usage gives the impression that the offender does not have to gain access necessarily to a computer system; she merely has to be in a position to gain access or have the capability of doing so. The question of being in a position to secure access must be considered in tandem with the intention to commit an offence. Given that this phrasing has not been given content by the legislator, it runs the risk of being too broad.

Consider, for example, an IT engineer who is examining the cybersecurity measures of her corporate client's computer system. Of course, she has authority to access the computer system on which she is working, but let us say that in doing so she stumbles upon a classified folder with incriminating data about the company. At this point, it may be said that she has overstepped her authority and is in a position to alter, modify or delete the data, copy or move the data, obtain the system's output data, or otherwise use the data. In terms of the element of unlawfulness, it is clear that she does not have the authority to act on her discovery of the incriminating and confidential data. The question here is, does the fact that she is in a position to alter, modify or delete data presume an intention to do so? In other words, can she be held liable criminally merely for being in a position to secure access without any determination that she has the intention of securing access? Upon a strict interpretation of this provision, it is conceivable that, in contentious circumstances, the specific intention to commit the offence might be overlooked. It would have been better to

54 Cybercrimes Bill [B 6B-2017], Explanatory Notes at 66.

leave out the phrase “in a position to” from the definition of securing access and require instead that the offender actually alters, modifies or deletes data and so forth. The conduct of the accused should not be judged on what she is capable of doing but rather on what she actually does.

Finally, the offence must be committed against a computer system in its various forms. This element sets out what the suitable target is and the provisions in section 2 of the Cybercrimes Act are sufficiently broad to cater for any and all forms of computer systems. They are broad enough also to cater for future technological advancements.

The manner in which these provisions have been drafted leave too much space for speculation and wide interpretation. They are formulated in a way that could see a person who is without criminal or malicious intent being classified as a motivated offender. Criminal liability could attach far too easily and possibly by virtue of unfortunate circumstances. Ultimately, if the people described in the examples above were to be prosecuted, their convictions would do nothing to give guidance regarding the social factors which allow for the successful commission of cybercrimes, simply because the true nature of the motivated offender would not be identifiable.

3.4.2 Multi-Coloured Hats: The Hacker

The punishable acts that are listed in section 2 of the Cybercrimes Act are sufficiently expansive to cover most possible modes of securing access to a computer system. In essence, the harm that this section is trying to guard against is any unauthorised and intentional interaction with a computer system. It addresses that concern relatively well.

It is now common cause that the biggest threats to computer systems are hackers. It was in the 1960s and 1970s that the hacker community came into being in the United States, with a counter-cultural ethic that was in line with the social and political values of the day. Some years ago, the word “hacking” was known only to an elite group of people who were active in the specialised world of computer technology. It was a label that had a positive connotation, describing the innovators and pioneers of the internet.[55] It was meant to denote a creative person who could manipulate and alter computer programmes

55 Yar (2005b) at 389.

and systems to perform functions that were beyond their inherent or intended design.[56] Today, the word has entered the everyday lexicon. Thus, taking everyday household objects and making them perform a different function from their original design is referred to as "life hacks". An example of this is using cold drink cans and fashioning a makeshift gas stove with them.[57]

The word "hacking" has undergone various transformations since its inception in the 1960s. Initially, as observed above, it was used to refer to someone who was highly skilled in developing effective and useful solutions to computer related problems. However, today hacking is associated with computer criminality and various forms of network intrusion.[58] Hackers are considered to be threats to network security in a society that increasingly is interconnected and dependent on computer technology.[59] Whereas there is no settled definition of the phenomenon in computer science and IT hacking is understood as gaining unauthorised access to a computer system and subsequently using it.[60] This is a basic definition that may be modified to fit specific circumstances. This means that it would be possible for one to find a legal definition of hacking that differs significantly from a definition in a cybersecurity report. However, it is expected that there would be many shared characteristics.

It is necessary to engage with the origins of the word "hacking" and the history of hackers because it helps to provide an informed perspective on the intentions and activities of today's hacker. This is because hacking has evolved from a culture underpinned by certain ethics and beliefs which are still relevant. It was a clearly defined ethic that was associated closely with youthful rebellion and protest movements.[61] It emphasised the right freely to access and exchange knowledge and information. Participants held the belief that the science and technology found in computers should be used to benefit and enhance the lives of all. Their ethical stance also reflected both a distrust of political, military and

56 Yar (2005b) at 388.
57 CrazyRussianHacker "10 Survival life hacks", available at https://www.youtube.com/watch?v=3owubdDJGmc.
58 Calo et al. (2018) at 1.
59 Gunkel (2005) at 595.
60 Richterich & Wenz (2017) at 5.
61 Muncie (1999) at 178-183; Taylor (1999) at 24–6; Thomas (2002).

corporate authorities and a resistance to "conventional" and "mainstream" lifestyles, attitudes and social hierarchies.[62]

Any attempt to offer a simplistic and all-encompassing description of computer hackers would be to commit a great injustice, as they are as diverse as they are many. However, there is some merit in classifying them into three camps, for a better understanding of who they are and how they operate as offenders. Hackers usually are classified by the colour of their proverbial hats, which is dependent largely on what they deem to be a suitable target for hacking: white hats, black hats and grey hats.

White hat hackers are known also by their professional title of penetration testers or ethical hackers and are on a quest to discover security weaknesses and vulnerabilities in the computer systems of organisations.[63] They may be hired by companies actively to hack into their computer systems in order to pre-empt attacks from black hat hackers.[64] They then participate in fixing the problems and developing better, more secure computer systems. One may enrol in courses to learn hacking skills as well as the ethics of hacking. White hat hackers are not considered to be offenders because they possess the necessary authority to gain access to the computer systems which they hack.[65]

Black hat hackers occupy the opposite end of the spectrum from white hats. Their motivations can range from hacking for revenge, sabotage or simple criminal gain (for example, to steal money, products or services).[66] Black hat hackers act with criminal intent.[67] Given the divergent definitions of the word "hacker" and the connotations it carries, the word "cracker" is sometimes applied to the black hat hacker and it delineates the stereotypical intruder who gains unauthorised entry into a computer system. Sections 2 and 3 of the Cybercrimes Act are designed to address the conduct of the black hat hacker. Their provisions would not apply to the white hat hacker because her actions would be authorised. While they can be applied clearly and easily to the black hat hacker, their relevance to the grey hat hacker would need to be examined carefully.

62 Yar (2005b) at 389.
63 See Marsh (2017) 5.
64 Falk (2004) at 1; Marsh (2017) at 4.
65 Security Trails (2018) at 1.
66 Schell, Dodge & Moutsasos (2002); Marsh (2017) at 5.
67 Marsh (2017) at 4.

Grey hat hackers may be found somewhere in the middle of the hacking spectrum. They typically hack for curiosity, fun, notoriety or self-fulfilment, but usually they do not seek to harm their targets nor act with criminal intent.[68] The concept of harm, however, is not an easy one to determine because it can be rather subjective and will differ substantially from the perspective of the victim or target as opposed to that of the offender. This is what makes drawing clearly defined lines between white, grey and black hats extremely difficult, if not impossible.

In many cases, grey hat hacking describes hacking exploits aimed at discovering security weaknesses in a computer system or in a product. Once those security vulnerabilities have been identified, they are brought to the attention of the owners (albeit often by public notice on a forum).[69] In many cases the hacker will do this for a reward. Grey hat hacking straddles the moral middle ground between white hats and black hats. While white hat hacking is an option for some, others may not be interested in working for corporations. Some may not be expert hackers but may stumble upon security vulnerabilities in certain systems and expose them without any criminal intent. Then there are those who use their specialised skills to make political statements. They are known as hacktivists.

Hacktivism is a relatively new phenomenon originating in the 1980s and gaining popularity in the 1990s and early 2000s. The word hacktivism is a combination of the terms hacking and activism and is generally described as the "nonviolent use of illegal or legally ambiguous tools in pursuit of political ends". [70] It is said to have been coined in 1996 by a member of the 'Cult of the Dead Cow', a group of hackers.

68 Xu, Hu & Zhang (2013) at 66. Although discussed by Xu, Hu & Zhang, the term Grey Hat hacker has not gained widespread adoption in the literature, most authors preferring to stick to the conventional white and black hat delineation.

69 Lemos (2002) at 1; Schiffer (2019) at 1.

70 Romagna (2020) at 743.

3.4.2.1 Anonymous

The word "hacktivist" has almost become almost synonymous with the loosely organised group called Anonymous.[71]

They proclaim:

> We are Anonymous
> We are legion
> We do not forgive
> We do not forget
> Expect Us

Members of Anonymous, or Anons as they are known commonly, believe that the ends always justify the means. This has led to their disregarding legal boundaries to protect their core beliefs, which include freedom of access to information and the right to unfettered self-determination on the internet.[72] They have perpetrated a host of incursions, from hacking into the servers of opponents, through orchestrating attacks and stealing companies' customer data, to pulling (often childish) pranks and knocking down or defacing websites. Some of the activities in which Anonymous has engaged attract hefty prison sentences, but its members always have felt secure in their online anonymity.[73]

3.4.2.2 Anonymous versus HBGary

The following discussion will recount the clash between Anonymous and cybersecurity firm HBGary[74] in order to highlight the complexity of classifying hackers by hat colour.

HBGary is an American cybersecurity firm that was started by Greg Hoglund and Aaron Barr in 2009. The firm specialise in design and distributions state-of-the-art computer forensics and malware art tools to the United States government as well as private institutions.[75] Hoglund already was running a security company called HBGary Inc when he approached Barr to start a sister company called HBGary Federal. The idea was that Barr

71 Notwithstanding the fact that recent years has seen a sharp decline in activities attributed to Anonymous mobilizing as a group, their impact on the birth and growth of hacktivism is unparalleled and as such warrants careful consideration.
72 Gyunka & Abikoye (2017) at 12.
73 Olson (2013) at 6.
74 Gyunka & Abikoye (2017) at 12.
75 Gyunka & Abikoye (2017) at 12.

could use his military background and cryptography expertise to sell services to the United States government.[76] In the beginning, the tiny company struggled but it stayed afloat by running "social media training" for company executives. These social media packages were not geared at teaching companies the ways in which to gain friends on Facebook or followers on Instagram, but were aimed at using these social media platforms to gather information about people as tools for spying.[77] These are typical services that a white hat security firm would provide to a client as they form part of social engineering.[78] HBGary was not an immediate success and to remedy his cash-flow problem, Barr decided to market his social media spying techniques by targeting Anonymous. This decision came on the back of the media attention that Anonymous had gained after *OperationPayback*, a 2010 hacking campaign against the websites of MasterCard, PayPal and Visa after these companies had decided to cut funding to Wikileaks.[79] Barr counted on the media attention around Anonymous to make a name for himself and HBGary.

In July 2011, Barr had been collecting data on members of Anonymous and he expressed his intention to release his findings at a San Francisco security conference. In the meantime, he was preparing to meet with FBI agents to reveal to them the identities of those he believed to be leaders of Anonymous during *OperationPayback*. In cybersecurity circles this is known as an act of "doxing". Some Anons became aware of this plan and subjected Barr and HBGary to a cyber-attack campaign which included taking over his Twitter account to post obscene tweets, defacing the HBGary websites and hacking his email server to steal a trove of emails which they made available online via torrents.[80]

Although HB Gary could have been classified as a white hat security firm on the face of it, some of its activities were shady at best and borderline illegal at worst. The leaked emails revealed that in October 2010, Aaron Barr had been in talks with Hunton & William, a law firm which had the US Chamber of Commerce and Bank of America amongst its clients. There had been hints from Wikileaks that it was in possession of a collection of confidential

76 Olson (2013) at 3.
77 Olson (2013) at 3.
78 Kaspersky Lab (undated) at 1 defines social engineering as "a form of techniques employed by cybercriminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites".
79 Addley & Halliday (2010) at 1; Gyunka & Abikoye (2017) at 13.
80 Olson (2013) at 6.

data on Bank of America. Hunton & William accepted presentations from cybersecurity firms about what approaches to take to deal with the rumours from Wikileaks. HBGary and two other cybersecurity firms gave presentations to Hunton & William. Some of their suggestions included disinformation campaigns to discredit Wikileaks, supporting certain journalists, and cyber-attacks on Wikileaks itself. Hunton & William appeared to be interested in HBGary's proposal although no contracts were signed.[81] In another deal, HBGary suggested to the Chamber of Commerce that it should engage in a similar campaign against the Chamber's political opponents, which included non-profit organisations and unions.[82]

Anonymous's attack upon Barr and HBGary was in retaliation against the supposedly dangerous misinformation that Barr had on Anonymous. The list of identities that Barr was planning to hand over to the FBI included names of people who were not affiliated to Anonymous but who may have been active on the public social media platforms where real members of Anonymous participated. Anonymous, assuming the roles of judge, jury and executioner, found Barr guilty of intentionally and negligently endangering the lives of innocent people who could face many years in prison for crimes they did not commit. On this matter — and many others — Anonymous felt that it held the moral high ground, which allowed it to pursue its opponents by whatever means necessary.

Of course, not all the Anons who participated in the attack on HBGary did so out of moral obligation. Some did it purely for the "lulz".[83] The lulz is essential in understanding the culture that is Anonymous. It involves a very weird sense of humour that may be palatable only to a group of weird individuals. *Wired Magazine* describes this as:

> the most important and abstract thing to understand about Anonymous, and perhaps the internet itself. The lulz is laughing instead of screaming. It's a laughter of embarrassment and separation. It's *schadenfreude* [pleasure derived from the misfortune of another person]. It's not the anesthetic humour that makes days go by easier, it's humour that heightens contradictions. The lulz is laughter with pain in it. It forces you to consider injustice and hypocrisy, whichever side of it you are on in that moment.[84]

81 Olson (2013) at 4.
82 Greenberg (2011) at 1.
83 The Lulz is a corruption of the LOL, a shorthand for laugh out loud typically used in social media platforms.
84 Norton (2011) at 1.

Anons who do not participate in a hacktivist campaign from a sense of moral indignation tend to do so for the lulz. Some who do it for the lulz do not need a better reason than that they think it would be funny — in the same way as a 13-year-old child might perform a prank that is not understandable to anyone else. This is not surprising, considering that the demographics of Anonymous and other hackers largely are dominated by young and immature boys in their teens and twenties. This behaviour is known as trolling which entails deliberately trying to enrage another internet user especially if they are taking something too seriously.[85]

Anonymous is a perfect example of hackers who straddle the headwear fence between white hats and black hats. Clearly, it is not a white hat group as it does not hold itself to ethical hacker standards, but by the same token it does not operate always with criminal intent. Given that Anonymous is not a structured organisation, a hat of a single colour cannot be ascribed to the group as a whole, because there are Anons on every node of the hacker spectrum. In order to deal effectively with a group like Anonymous, one needs to consider the individual intentions or motivations of the hacker. In this regard, one must employ the Routine Activities Theory (RAT) and engage with the motivated offender.

The Anonymous hacks and the leaked emails revealed the dubious activities in which the so-called white hat firm had been engaged, demonstrating that it is quite easy to wear different hats. While some of the firm's activities were not illegal, its behaviour showed the blurred lines between hacking categories, necessitating an evaluation of the motivations of the offender.

3.4.2.3 Project Chanology

In January 2008, a video surfaced on the internet of an interview with actor Tom Cruise in which he claimed that:

> we are the authorities on getting people off drugs, we are the authorities on the mind, we are the authorities on improving conditions ... we can rehabilitate criminals ... we can bring peace and unite communities.[86]

85 Galli (2018) at 14.
86 Barkham (2008) at 1.

Cruise was talking about the Church of Scientology. This video was an internal video produced by the Church of Scientology and when it surfaced on YouTube, the Church made efforts to have it removed as it was considered embarrassing.

Members of Anonymous, were enraged by this attempt by the Church to suppress the video and, thereby, to police the internet. To them, an attempt to censor the internet is an attack on freedom of speech[87] and a cardinal sin. This gave birth to the so-called Project Chanology, which was accompanied by the call for online and offline protest action against the Church of Scientology.

Because Anons believe in freedom of the internet and freedom of access to information, they were opposed to what they viewed as an attempt at suppression of free speech on the internet by the Church. They took this stance because the Church is infamous for being overly litigious and suppressive of critical voices against it, making use of copyright and trademark laws to do so.[88] The Anons launched a cyber-attack campaign against the Church. Project Chanology catapulted Anonymous into mainstream notoriety and cemented its reputation as a hacktivist organisation.

Soon after the video was repeatedly removed from the internet, Anonymous released a video to rally the troops so to speak, (below is a transcript of the video):

> Over the years, we have been watching you. Your campaigns of misinformation; suppression of dissent; your litigious nature, all of these things have caught our eye. With the leakage of your latest propaganda video into mainstream circulation, the extent of your malign influence over those who trust you, who call you leader, has been made clear to us. Anonymous has therefore decided that your organization should be destroyed. For the good of your followers, for the good of mankind--for the laughs--we shall expel you from the Internet and systematically dismantle the Church of Scientology in its present form. We acknowledge you as a serious opponent, and we are prepared for a long, long campaign. You will not prevail forever against the angry masses of the body politic. Your methods, hypocrisy, and the artlessness of your organization have sounded its death knell....
>
> You cannot hide; we are everywhere.

87 Galli (2018) at 15.
88 Barkham (2008) at 1.

> We cannot die; we are forever. We're getting bigger every day--and solely by the force of our ideas, malicious and hostile as they often are. If you want another name for your opponent, then call us Legion, for we are many....
>
> Knowledge is free.
>
> We are Anonymous.
>
> We are Legion.
>
> We do not forgive.
>
> We do not forget.
>
> Expect us.[89]

Project Chanology, also known as Operation Chanology, consisted of numerous activities that included prank phone calls to the Scientology Dianetics hotline, both to annoy and to disrupt service; ordering hundreds of pizzas to be delivered to the Scientology building; and online Distributed Denial of Service (DDoS) attacks on the Scientology website.[90] Some of the protest action against Scientology translated to the real world when members were encouraged to avoid illegal means by a man named Mark Bunker on 26 January 2008. They were urged to go to their nearest major city and protest the offices of Scientology on 10 February 2008. It has been reported that over 7, 000 protesters appeared across multiple major cities around the world.[91]

The people who were involved in Project Chanology engaged in the protest action for various reasons and with different capacities. One person who was arrested for his participation was Brian Mettenbrink. He was sentenced to a year in prison and ordered to pay $20 000 in compensation to the Church. According to reports, the activities of Mettenbrink and other members of Anonymous were likened to "hate crimes", for which they were arrested and punished.[92]

89 Galli (2018) at 15.
90 Anonymous Documentary (2014) at 22:32 minutes.
91 Galli (2018) at 15.
92 Leyden (2010) at 1.

Brian Mettenbrink participated in Project Chanology via a DDoS attack by using the Low Orbit Ion Cannon (LOIC, pronounced *Lo-ick*). LOIC[93] was an open source software that was free to use and downloadable on 4Chan (the site where Anonymous originated).[94] It worked in the same way as a botnet, except it was considerably less powerful, the difference being analogous to that between a long-range missile and a handgun.[95] Unlike a botnet, which takes over thousands of zombie computers to participate in a DDoS attack, LOIC depended on the participation of individual hackers. It was very easy to use and did not need to be monitored. If someone wanted to use it, she could instal it on her computer following a few easy instructions, input the relevant information and let it run in the background of her computer while she busied herself with other matters.[96] This is what Mettenbrink did. All things considered, his participation in Project Chanology was comparable to bringing a cup of water to the ocean.

At the time of the 2008 attack on the Church of Scientology, Mettenbrink was 18 years old and had heard about the attack from the social media site 7Chan (an associated site to 4Chan). Mettenbrink did not have any specific feelings about Scientology or the reasons behind the attack. His interest was in learning about IT security and he reasoned that taking part in this attack would give him an opportunity to learn about the other side of the industry.[97] He was a casual participant in Project Chanology, in the sense that his participation only went as far as the LOIC software. He was not a participant in the Internet Relay Chat (IRC) channels dedicated to the attack, such as *#xenu*, nor did he make any effort to find out when the next attacks would take place. He was a passive participant at best. After installing the LOIC software, he allowed it to run in the background of his computer and he eventually forgot that it was running. Three days later, he noticed that his internet connection had slowed down because of the software, so he decided to disconnect it.[98] Often, people used LOIC without knowing that it was illegal and therefore let it run directly off their computers without anonymising themselves, leaving their IP addresses exposed. This is how Mettenbrink was caught.

93 Gyunka & Abikoye (2017) at 12.
94 Olson (2013) at 79; Galli (2018) 13.
95 Olson (2013) at 79.
96 Olson (2013) at 79.
97 Olson (2013) at 81.
98 Olson (2013) at 81.

Although Mettenbrink was naïve in his participation, it was appropriate for him to be prosecuted for his participation in Project Chanology, but the sentence he was given was disproportionate to his crime. Mettenbrink was misguided in his participation in the attack and his role was insignificant. The sentence appears to have been exemplary, rather than aimed at punishing him for his offence. A proportional and appropriate sentence would have taken into consideration his motivation as an offender and possibly imposed upon him a small fine rather than a prison sentence of a year and a fine of $20 000.

The Mettenbrink case clearly shows that hacking is shrouded in myth. The abilities of hackers often are overstated, which adds to misinformation and sometimes irrational fears about them. Many hackers, like Mettenbrink, are script kiddies, who hack into systems out of curiosity and misguided actions easily attributable to youthful insouciance. This is not to say that there are no dangerous and threatening cybercriminals. There are plenty, but not as many as usually imagined.

Pursuing script kiddies like Mettenbrink with the full force of the law does two unhelpful things. Firstly, it wastes valuable resources that could be spent on investigating, arresting and prosecuting the really skilled and dangerous hackers. For Mettenbrink to spend a year in prison does absolutely nothing to reduce the overall level of cybercriminality. Secondly, Anonymous derives its power from its numbers. Its slogan, reproduced at the head of this section, indicates its sense of untouchability. The line "We are legion" makes reference to the Bible passage where Jesus Christ asked the man with the unclean spirit what his name was. The man replied: "My name is legion for we are many."[99] The headless suited man icon of Anonymous represents a legion of people acting as one. This means that arresting some Anons will do little to stop Anonymous. If anything, it very well may be infighting that has slowed its momentum, rather than fear of arrest and prosecution.

It is well known that Mettenbrink and others arrested after Project Chanology are small fish in the greater scheme of Anonymous activities. This means that the authorities, by not taking into account the intentions and realistic roles that hackers play in these attacks, in fact reinforce the idea of Anonymous being untouchable, as the script kiddies become the

99 The Holy Bible: Book of Mark, Chapter 5, Verse 9.

sacrificial lambs while the dangerous hackers who know how to cover their tracks remain beyond the reach of the law. In the meantime, valuable resources are being depleted to win minor victories.

How effective sections 2 and 3 of the Cybercrimes Act will be will depend on a thorough understanding of the hacker culture. This issue necessitates an engagement with the motivations of the hackers, in order to determine which colour hat an individual is wearing.

3.4.3 Hacking and the Cybercrimes Act

Anonymous enjoys a presence globally, as well as locally in South Africa. We have not been immune from hacktivist attacks.[100] In 2016, it was reported that Anonymous, under the banner of Anonymous Africa, launched an attack on the websites of the South African Broadcasting Corporation (SABC) and the Gupta-owned entity, Oakbay Investments.[101] A different group of Anons, working under the banner of Operation Africa, hacked the website of the South African government-owned arms supplier, Armscor, and proceeded to leak Armscor data on the dark web. It is reported that the files that were leaked included ordering and payment details for a number of companies associated with Armscor, including Airbus, the Thales Group, Rolls Royce and Denel. In addition, the hacktivists appear to have gained access to the identity numbers, names and passwords of some of Armscor's suppliers.[102]

According to section 2 of the Cybercrimes Act, if it were possible to identify specific people responsible for the attack on Armscor, a number of matters would have to be determined in order to establish their liability. The first is whether or not there was intention to secure access to the computer system. Much of the Anonymous rhetoric revolves around the insistence that Anons are not hackers but rather that they are hacktivists. This distinction points to their motivations, which they could raise as a ground of justification, but which are irrelevant in determining whether there was intention to secure

100 *News24* (2015) at 1; Vermeulen (16 February 2016) at 1; Vermuelen (13 June 2016) at 1; Van Zyl (25 July 2016) at 1; *Daily Maverick* (2016) at 1; Cowen (2016) at 1.
101 Van Zyl (2016) at 1.
102 Van Zyl (2016) at 1.

access to a computer system. This is in keeping with RAT, which takes the offender's proclivity to offend as a given.

The second issue is whether the access was unlawful, and in this case it was obviously an unauthorised breach. The third issue relates to the identity of the suitable target. The first target was the data that Anonymous stole from Armscor and leaked on the dark web. The applicable provision of the Cybercrimes Act would be section 2(1)(a), which stipulates that "any person who unlawfully and intentionally accesses data is guilty of an offence". The second target was the Armscor website itself, meaning that the attack would fall under section 2(2)(b)(iv) of the Cybercrimes Act, which provides that "a person accesses a computer programme when the person is in a position to obtain its output". The output in this case would be the stolen and leaked data. This provision is most appropriate when there is an attack on a website and data has been stolen. Where there is a DDoS attack or when a website has been defaced, as in the attack against the SABC and Oakbay Investments, sections 5 and 6, which deal with unlawful interference, are better suited.

Section 3 of the Cybercrimes Act is related closely to section 2. Section 3 prohibits the unlawful and intentional interception of data which includes electromagnetic emission from a computer system carrying such data. Interception of data means the acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool so as to make it available to someone who is not the lawful owner or holder of the data, nor the sender or (intended) recipient of the data. This prohibition includes the examination or inspection of the contents of the data and the diversion of the data to a different destination from what was intended.[103] Section 3 of the now superseded version [B6—2017] prohibits acquiring data unlawfully. This means to use data, examine or capture data or any output thereof, copy data, move data to another location in the computer system in which it is held or to any other location, or to divert data from its intended destination to any other destination.[104] The two provisions — the earlier and the current — differ slightly in their formulation but they are fundamentally similar.

The current section 3 of the Cybercrimes Act is directed at protecting the confidentiality and integrity of a computer system, and thus complements section 2 by

103 Section 3 of the Cybercrimes Act.
104 Section 3(4) of the Cybercrimes Act.

prohibiting any act aimed at overcoming any measure intended to prevent access to data. It also prohibits the unlawful interception or acquisition of data which is transmitted to or from a computer system. This provision goes further than section 2 and those sections dealing with the other hacking offences, as it explicitly makes it an offence for one to possess data which one knows has been intercepted unlawfully.

3.5 Interference

Interference with a computer system can be an attack upon its integrity and availability, that is, the second and third elements of the CIA triad. The chief aim of interference attacks is to ensure that individuals, businesses and government structures do not have any of their systems functioning optimally. Without constant availability, there is a risk of considerable pecuniary damage and disruption to public administration.[105] Sections 5 and 6 of the Cybercrimes Act try to protect against these risks.

The Budapest Convention, in Articles 4 and 5, provides for data interference and system interference respectively. Article 4 prescribes that each Party shall adopt legislation that criminalises unlawful and intentional damaging, deleting and deteriorating, altering or suppressing of computer data. Said Party may reserve the right to require that the conduct result in serious harm. Article 5 provides for the criminalisation of conduct which unlawfully and intentionally causes:

> serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

The aim of this provision is to give protection to incorporeal objects in a way similar to protecting physical objects against intentional infliction of damage.[106]

In terms of Article 5, the acts of deteriorating and damaging computer systems are overlapping acts in how they relate to causing negative changes to the integrity of a computer system. To suppress computer data means to render the data inaccessible from the computer system or the server where it is stored. The alteration of data means its modification.[107] Hindering refers to actions that interfere with the proper functioning of a

105 Cybercrimes Bill [B 6B-2017], Explanatory Notes at 66.
106 Budapest Convention, Explanatory Report at 65.
107 Budapest Convention, Explanatory Report at 66.

computer system. It can occur by inputting, transmitting, damaging, deleting, altering or suppressing computer data. The legal interest which this provision is protecting is the availability of the computer system. It seeks to do so by criminalising the intentional hindering of the lawful use of the computer system, and includes the protection of telecommunication systems.[108]

Sections 5 and 6 of the Cybercrimes Act closely follow the wording of the Budapest Convention. These sections are also fundamentally similar to sections 2 and 3 in that they address hacking offences. However, sections 5 and 6 address interference with a computer system whereas sections 2 and 3 address unauthorised access to a computer system.

Section 5 makes it an offence unlawfully and intentionally to interfere with data or a computer programme. It provides that conduct is considered to be an act of interference if it temporarily or permanently deletes, alters, renders vulnerable or meaningless, damages or deteriorates, obstructs, interrupts or interferes with or denies access to data. This provision is straightforward in what it sets out to do. The *mens rea* element is intention and the interference must be unlawful. The interference may be either temporary or permanent. There is no minimum time set out in the Act nor the explanatory notes to specify how long temporary is, which is not surprising because interference with data or a computer programme could result in varying degrees of damage occurring. Take, for example, the damage that could result from interfering with the website of a multinational company for a single hour and compare it to shutting down Plain Jane's blog about gardening for an entire week. Depending on the aim of the motivated offender, the duration of the interference can be insignificant.

Unlike section 5, section 6 of the Cybercrimes Act focuses not on data or a computer programme but on a computer data storage medium or a computer system. In section 6, interference means temporarily or permanently altering any resource of or interrupting or impairing the functioning, confidentiality, integrity or availability of a computer system or computer data storage medium. The section refers to the elements of the CIA triad, highlighting them as key aspects of interference. While interference can cause a disruption in the confidentiality and the integrity of a computer system, so can unlawful access. A

108 Budapest Convention, Explanatory Report at 65.

better indicator of the challenge of interference may be observed clearly in relation to the availability element of the CIA triad. The DDoS attack is an excellent example.[109]

Section 5(2)(f) provides that interference with data or a computer programme means permanently or temporarily to deny access to said data or programme. Section 6(2)(b) provides that:

> Interference with a computer data storage medium or a computer system means permanently or temporarily to interrupt or impair the functioning of; the confidentiality of; the integrity of; or availability of a computer data storage medium or a computer system.

Both sections 5 and 6 speak directly to the DDoS attack. There are numerous other types of attacks that may be subsumed under these provisions, but the DDoS attack is one of the more popular in hacktivist circles and will be used to illustrate the effectiveness of these provisions.

Simply put, a DDoS attack involves overwhelming a targeted network or computer with network traffic from innumerable locations all over the world. The aim of the attack is to prevent the network from performing its normal work.[110] It is characterised by an explicit attempt to obstruct the legitimate use of the service.[111] It does this by deploying multiple attacking entities which assault the target with a stream of malicious traffic which may cause it to suffer damage. Some have argued that DDoS attacks are modern versions of a sit-in protests.[112]

There are various ways in which a DDoS attack may be performed. The first involves the attacker sending a stream of traffic to the victim's network, thereby consuming some of the key resources of the network and rendering it unavailable to legitimate users.[113] It is common that a botnet would be used in this regard. The second approach involves the attacker sending malformed packets to the victim's network. This would cause an application or a protocol on the victim's computer to be confused by the commands that it is receiving and thereby provoke it to freeze or reboot.[114] These approaches are by no

109 A Denial of Service (DoS) attack transmutes into a Distributed Denial of Service (DDoS) attack when it comes from a great number of sources rather than from a single source.
110 Lepofsky (2006) at 40.
111 Mirkovic & Reiher (2004) at 39.
112 Galli (2018) at 16.
113 Romagna (2020) at 12.
114 Mirkovic & Reiher (2004) at 40.

means the only ways in which service can be denied on the internet, but they are the most common.

It does not make a significant difference whether a motivated offender is securing access to a computer system or if she is interfering with it. She still would be referred to as a hacker. The difference between a person who secures access and one who interferes lies in what is deemed to be a suitable target. It was noted in the previous chapter that the suitability of a target is determined from the perspective of the offender. Where one offender may access data or a computer programme to steal or leak it, another may interfere with data or a computer programme to make some kind of (political) statement.

This may be observed from the type of harm that results. When an offender steals data, she is able to sell it on the deep web and make money for herself or for the entity for which she works. The target from which she has stolen the data does not lose money necessarily, because the offender may have duplicated the data, without dispossessing the target. In other words, if an offender steals a target's identity number by gaining access to a company database, the target may not experience any pecuniary loss from that theft *per se*, whereas the offender will gain a financial benefit from selling the identity number. Conversely, in the case of interference, the offender most likely would not receive a financial benefit from the conduct, aiming instead to cause the target to lose money. Take, for example, the defacement of a website by altering or deleting data, which might cause confusion for the target's clients or cause embarrassment to the target, resulting in the loss of trust and, therefore, investments. The difference between the two is nuanced and may not be especially significant because, in most cases, the two tend to co-exist and reinforce each other, since, for an offender to interfere with a computer system, she needs to secure access to it first. Nevertheless, it is important to note the differences because they may give an indication of the social factors that are present and highlight the reasons why a motivated offender may find one target more suitable than another and why she might choose to perpetrate her offence in a particular way.

3.6 Cyberforgery and Uttering

The Cybercrimes Act has two provisions which deal with the crime of fraud. The first is section 8 which addresses the crime of cyberfraud and the second is section 9 which

addresses the crime of cyberforgery and uttering. In both offences, the *mens rea* is the intention to defraud. They differ as regards the *actus reus.* This difference in the *actus reus* is what makes one of the offences a true cybercrime and the other not. Cyberforgery and uttering is a Type I offence whereas cyberfraud is a Type II offence. The latter will be discussed in Chapter Four, as it is a computer enabled crime and therefore is not a true cybercrime.

This section discusses the crime of cyberforgery and uttering. Cyberforgery is the act of making false data or a false computer programme which results in actual or potential prejudice to another person. Cyber uttering entails passing off false data or a false computer programme to the actual or potential prejudice of another person. Although both these offences may be committed offline without reliance upon the internet, technological advances and offender ingenuity have made them significantly distinguishable from offline offences. That is to say, they have assumed an identity which elevates them from being computer enabled to being computer dependent. To be sure, this does not mean that there are no longer instances of offline forgery and uttering, but rather that there is a need to create a cybercrime of forgery and uttering. By way of illustration, phishing and pharming will be discussed in relation to this offence.

Article 7 of the Budapest Convention makes provision for computer-related forgery. It provides that parties should adopt legislation which criminalises conduct where input, alteration, deletion or suppression of computer data results in the creation of inauthentic data which the offender intends to be considered or acted upon for legal purposes as if the data were authentic, whether or not readable and intelligible. The provision leaves it to the individual Party to decide whether it requires an intent to defraud, or similar dishonest intent, before attaching criminal liability.

Article 7 of the Budapest Convention casts a wider net of liability than section 9 of the Cybercrimes Act. The *mens rea* is not limited to an intent to defraud but allows for criminal liability to attach also to “similar dishonest intent”, which presumably would be determined by the presiding judge. Furthermore, the Convention does not require that the inauthentic data be directly readable and intelligible. One may assume that this would apply to malicious code which is written by hackers and would not necessarily be readable and intelligible to the target but would be able still to achieve its desired result.

Section 9 of the Cybercrimes Act addresses the creation of mechanisms which would allow an offender to defraud a target. The type of fraud which is applicable to this section is personal fraud, that is, fraud which is directed at individuals. Personal fraud may be divided into two categories: consumer scams and identity fraud. A consumer scam may be understood as:

> a fraudulent invitation, request, notification or offer, designed to obtain someone's personal information or money, or otherwise obtain a financial benefit by deceptive means.[115]

By contrast, identity fraud involves "the theft of an individual's personal details without their [sic] consent and includes both identity theft and credit or bank card fraud".[116]

Of course, both these forms of fraud are still active in the offline environment, as will be seen in the discussion of cyberfraud later, but technological advancements play an important role. The discussion here is not necessarily about the suitable target being defrauded by the motivated offender but rather about the techniques or tools that the motivated offender uses to defraud the suitable target. Cross *et al* define online fraud as:

> the experience of an individual who has responded via the internet to a dishonest invitation, request, notification or offer by providing personal information or money that has led to a financial or non-financial loss or impact of some kind.[117]

There are many different types of online fraud scams but most of them involve advance fee schemes — such as the lottery fraud, romance scams and inheritance schemes — which carry the promise of a reciprocated benefit for the transfer of funds.[118] These do not fall within the ambit of section 9 of the Cybercrimes Act. The section concerns those types of online fraud that seek to obtain sensitive personal information, such as bank account details or verified identity information, enabling the offenders to withdraw money from the victims' accounts without their knowledge,[119] through the abuse of the internet and computer systems. Identity theft (which for these purposes encapsulates personal data theft) will be the focus of this discussion.

115 Australian Bureau of Statistics (ABS) 2012.
116 Australian Bureau of Statistics (ABS) 2012.
117 Cross *et al* (2014) at 1.
118 Cross *et al* (2014) at 2
119 Cross et al (2014) at 1; Viliç (2019) at 44.

The two most common forms of identity theft for the crime of cyberforgery and uttering are phishing and pharming. In essence, phishing uses bulk emails or spam emails to entice the target into divulging personal information. Pharming clandestinely installs malware into the target's computer system. The malware thereafter misleads the target by diverting her web searches from legitimate websites to fake websites where the personal information is harvested.[120]

Identity theft occurs when the motivated offender obtains confidential information from a suitable target in order to gain access to her financial records or other sensitive and valuable data. The stolen identity information, such as identity numbers, residential addresses and dates of birth or answers to common security questions, can be used to open fraudulent bank accounts in the name of the target, take out hefty loans and make expensive purchases.[121] This typically leaves the target with debts that she cannot account for and very limited avenues of legal recourse.

The targets of identity fraud are not limited to individuals — businesses can fall victim to this crime also. In the case of businesses, identity theft may not be directed at the business itself but rather at its clients. Identity thieves may find it easier to attack the data centres of a business and steal the clients' personal information in bulk rather than from one individual at a time. A serious and adverse effect that the business may face is a loss of trust from its clients, as it may become seen as unreliable and insecure.[122] This fear also increases the chances of a business not disclosing cases where its security systems have been breached, leading to under-reporting and victims being unaware that they have been compromised.

3.7 Ancillary Offences

The offences that will be discussed in this section have been categorised as ancillary offences because they can be committed only as accessory to the core hacking offences discussed above.

120 Viliç (2019) at 46 - 47.
121 Brody *et al* (2007) at 43.
122 Brody *et al* (2007) at 44.

3.7.1 Section 4 of the Cybercrimes Act

Section 4 provides for offences in respect of software or hardware tools. It prohibits unlawfully and intentionally using or possessing any hardware or software tools which can be used to commit any of the hacking offences described above, that is, unlawful access (in terms of sections 2(1) and 3(1)) and unlawful interference (in terms of sections 5(1) and 6(1)). It also criminalises these acts when committed in terms of section 7(1)(a) or (d). Version [B6-2017] is wider as it also criminalises the manufacturing, assembling, obtaining, selling, purchasing, making available or advertising of any software or hardware tool. A software or hardware tool is defined as any electronic, mechanical or other instrument, device, equipment, apparatus or substantial component of such a device or computer programme, which is designed or adapted primarily to contravene the abovementioned provisions.[123]

According to its explanatory notes, the Cybercrimes Act recognises that there are certain tools that are not necessarily unlawful in their usage. They might have dual usage — for example, encryption software which can be used not only to keep confidential information safe but also to launch ransomware attacks. In order to avoid over-criminalisation of these tools, the Act has adopted the approach, taken in various national and regional benchmarks, to require that there should be specific intent to commit certain unlawful offences.[124] Section 4 is straightforward and uncontroversial.

3.7.2 Section 7 of the Cybercrimes Act

Section 7 is concerned with an ancillary offence relating to passwords, access codes and the like. As seen above, section 4(1) makes reference to it, but this does not elevate it to the status of a core crime. Rather, it finds applicability in terms of the core crimes contained in sections 2(1), 3(1), 5(1), 6(1), 8 and 9(1). The section 7 offence consists in intentionally and unlawfully acquiring, possessing, providing, receiving or using passwords, access codes or similar data or devices to commit the aforementioned offences. This offence also extends to anyone who is found in possession of any passwords, access codes and the like where there

123 Section 4(2) of the Cybercrimes Act.

124 The Cybercrimes Bill [B 6B-2017], Explanatory Notes at 66.

is reasonable suspicion that such were acquired, possessed, provided or used to commit the offences.

Section 7(3) defines passwords, access codes or similar data or devices as including but not limited to the following:

> (a) a secret code or pin;
> (b) an image;
> (c) a security token;
> (d) an access card;
> (e) any device;
> (f) biometric data; or
> (g) a word or a string of characters or numbers,
> used for—
> (i) financial transactions; or
> (ii) user authentication in order to access or use data, a computer programme, a computer data storage medium or a computer system.

This definition is formulated expressly "without limitation". The inclusion of the phrase "without limitation" is to be welcomed because it acknowledges the development of technology and the possibilities that exist in the future of cybercrime.

3.7.3 Section 10 of the Cybercrimes Act

Section 10 provides for an interesting offence of cyber extortion. This offence finds its most appropriate expression in the mushrooming phenomenon on ransomware.

3.7.3.1 The Evolution of Ransomware

Ransomware is not a new phenomenon — it has been around since the late 1980s and it has evolved in true Darwinian style. In its early life, ransomware was not successful widely, given the landscape into which it was born, that is, an era when computers were not ubiquitous and the internet was still a concept and accessible only to Universities, research entities and governments. Additionally, in those days, international payments were much harder to execute than they are now. Furthermore, that era saw malware being used for vandalism, pranks and notoriety rather than for financial gain.[125]

Fake antivirus scams became very prominent in 2008 and 2009, seeking to trick victims into believing that their computer systems had been infected with a virus and they needed to buy the antivirus that is being offered to them to remove it. Fake antivirus scams

125 Savage, Coogan & Lau (2015) at 7.

worked in a manner similar to locker ransomware (discussed below) in that it would prevent access to the computer system. The attack relied heavily on social engineering techniques to trick the victim into thinking that her computer has been infected with a virus and that this antivirus which had detected it would be able to clean the computer.[126] She therefore would be more likely to trust in the "antivirus" that has detected the problem. After downloading it, the "antivirus" would offer the victim an option to purchase a subscription of the "antivirus" at a supposedly low price, whilst infecting the computer with a real virus.

It was in early 2005 that the first wave of modern crypto ransomware (discussed below) threats began to surface. One of the earliest forms was the *Trojan.Gpcoder* family of viruses which did not use a strong form of encryption technology, was easily overcome and, therefore, was not very successful. It used symmetric encryption which meant that the encryption and the decryption keys were the same. However, the authors of the malware were not deterred easily and they continued to adjust the malware to produce newer and more effective versions.[127]

The first pure locker ransomware appeared between 2011 and 2012 in the form of *Trojan.Randsom.C*, which operated by requesting the user to call a premium-rate phone number to a spoofed Windows Security Centre in order to reactivate the licence to the security software.[128]

Crypto ransomware is the original type of ransomware and, with the deficiencies of the locker ransomware becoming evident, there has been a move back to crypto ransomware since 2013. Crypto ransomware is different from locker ransomware in that it does not see the need to use social engineering to trick the victim into complying with its demands. It is direct in approach and makes the victim aware from the onset of its intentions.[129] Crypto ransomware can demand as much as US$300 for a single computer to be decrypted.

126 Savage, Coogan & Lau (2015) at 9.
127 Savage, Coogan & Lau (2015) at 9.
128 Savage, Coogan & Lau (2015) at 9.
129 Savage, Coogan & Lau (2015) at 11.

3.7.3.2 The Nature of Ransomware

As appears from the discussion above, there are two main types of ransomware. The first is locker ransomware which prevents access to a computer or device by locking the computer or device itself. The other is a crypto ransomware which prevents access to data or files by locking or encrypting the data itself rather than the computer or storage device that houses it. Whereas it does not necessarily have to use encryption to lock the data, much of this type of ransomware does.[130]

Locker ransomware usually locks the victim's computer or the computer interface and then asks the victim to pay a fee to unlock it or restore access to it. It can limit the functioning of a computer, for example, by preventing the mouse from working or leaving only the numeric functionality of the keyboard (to allow the user to enter the payment code once the ransom has been paid). The underlying system of the computer is left untouched, which means that it is possible for a skilled cybersecurity expert to remove the malware and restore the computer to full functionality.[131]

Social engineering is one of the techniques that is relied upon heavily when a locker ransomware attack is perpetrated. It is necessary to enlist manipulation and deception techniques against unsuspecting victims because the malware itself is relatively easier to remove than in the case of crypto ransomware.[132]

A common technique which offenders use is to produce a pop-up notice on the victim's computer which masquerades as a law enforcement notice. In many cases, the victim receives a notification which purports to be from the US Federal Bureau of Investigation (FBI) and informing her that the FBI has detected that her IP address has been linked with downloading or visiting a website which hosts child pornographic material, abuse of children, zoophilia or material related to terrorist activities. These are federal crimes in the United States and carry a prison sentence of up to twelve years. She is informed that she is required to pay a fine immediately to avoid arrest and prosecution. She

130 Savage, Coogan & Lau (2015) at 5.
131 Savage, Coogan & Lau (2015) at 5.
132 Savage, Coogan & Lau (2015) at 5.

is then instructed to follow certain commands that will enable her to pay the fine.[133] After she pays, the malware presumably will be removed, although that typically is not the case.

Unlike locker ransomware, crypto ransomware is designed to find and encrypt valuable data on the victim's computer or storage device. Valuable data can range across anything, including personal information, photographs, company documents and confidential government documents. The data will be made inaccessible to the victim and the decryption key is in the possession of the offender alone. Crypto ransomware exploits vulnerabilities in computer systems to gain access to the data. It can operate in the background of the computer system, for as long as is necessary for the valuable data to be encrypted, without being detected by any protective measures which the victim might have, such as firewalls or antivirus software. The ransomware thereafter presents a message to the victim informing her that her computer has been infected with ransomware and that she needs to pay an amount for having the decryption key released to her. By the time she receives this notification, all her data would have been encrypted and there is very little that she can do to stop the attack or recover her data.[134] Bitcoin or any other type of cryptocurrency is usually the preferred payment method because of its security, anonymity and relative untraceability.

In the early days of crypto ransomware, the affected computer usually could continue to function normally, as the malware would not target the critical system files of the computer, only barring access to the encrypted data.[135] The modern-day ransomware attacks can encrypt the computer all the way to the hardware level, making it near impossible to unlock without a decryption key.

May 2017 saw a cyber-attack that was unprecedented in scale globally. *WannaCry* — a crypto ransomware variant which is known also as *WannaCrypt, WanaCrypt0r, WRrypt* and *WCrypt* — was introduced through a phishing email and once it had entered the computer, it used a Windows vulnerability to replicate itself and spread from the first infected computer to the rest of the network.[136] From this, it was immediately clear that the targets of the ransomware were not individual home users but rather organisations or

133 FBI (2012) at 1.
134 Savage, Coogan & Lau (2015) at 7.
135 Savage, Coogan & Lau (2015) at 7.
136 Europol (2017) at 1.

entities who had their computers connected on a network. This kind of large scale attack is desirable to the attacker because it provides her with a greater pool of victims and, therefore, a greater capacity to secure a greater ransom.

It is estimated that the attack affected at least 99 countries, with Russia being the worst hit. The *WannaCry* ransomware attack held ransom computer data of hospitals, telecommunications firms[137] and car manufacturers,[138] to name a few. The United Kingdom suffered immensely from the attack, as it crippled the National Health Service (NHS) for a considerable period of time. The effect that the ransomware had on the NHS was a cause for great concern because it froze computers at hospitals around the country, which resulted in the forced closure of many hospital wards. British citizens were advised to report to the A&E department of the hospitals only in emergencies.[139] It was reported, however, that patient information had not been compromised,[140] although patients were affected negatively by the attack — one patient reported that his scheduled heart surgery had to be postponed due to the attack.[141]

The *WannaCry* ransomware attackers demanded a ransom of $300 from each of the individual computers infected with the malware, failing which the ransom amount would double in three days. Further, if the ransom were not paid, the data would be destroyed.[142] It spread at an exponential rate on the day it was released before it was halted by a "kill switch" discovered by cybersecurity researcher, Marcus Hutchins. Ironically, Hutchins was arrested two months later, while he was in the US, for writing and distributing a banking Trojan malware which was used on one of the bigger dark web marketplaces, AlphaBay.[143] This charge is unrelated to the *WannaCry* ransomware outbreak.

The speed at which the ransomware attack propagated and its wide spread were cause for great concern, because they highlighted the great capability of cybercrime to be far-reaching and destructive. To date, Africa has not experienced ransomware attacks on the scale that Europe and America have, but it is only a matter of time before it does.

137 CBS News (2017) at 1.
138 Sharman (2017) at 1.
139 CBS News (2017) at 1.
140 BBC (2017) at 1.
141 CBS News (2017) at 1.
142 CBS News (2017) at 1.
143 Shugarman (2017) at 1.

Ransomware attackers have shown that they do not respect national boundaries. Although South Africa did report a handful of cases during the *WannaCry* attack of 2018, those cases were not enough to cause alarm. This, however, will not remain the position indefinitely, as another large-scale (even worldwide) ransomware attack is inevitable. Fortunately, when one considers South Africa's readiness for such an attack from a legal perspective, section 10 of the Cybercrimes Act comes close constituting an effective response.

3.7.3.3 Ransomware and the Cybercrimes Act

Section 10 criminalises cyber extortion. It provides that:

> 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.

The cyber extortion section includes an additional element of intent, which requires that the perpetrator act with the purpose of "obtaining any advantage from another person" or "compelling another person to perform or abstain from performing any act". Essentially, cyber extortion requires special intent. The special intent element is desirable because it highlights the fact that different cyber acts may be classified differently according to their gravity. This is also important when it comes to sentencing, particularly in cases involving aggravated circumstances, where it provides necessary flexibility. Therefore, to understand this offence, it is necessary to read it together with the hacking offences in sections 3(1), 5(1), 6(1) and 7(1)(a) or (d) of the Cybercrimes Act.

The dependence of section 10 upon the core crimes makes it an ancillary offence. While the other ancillary offences are straightforward and need not be unpacked, cyber extortion recently has gained popularity and therefore is worthy of comment. An offender who gains access to a computer system to send spam and an offender who gains access to launch ransomware occupies the terrain of different classes of cybercrimes in relation to the impact on victims. Although both hacking offences and ransomware attacks involve unlawful intrusion into a computer system, their differing impact dictates that they should not be treated in the same way. It is important for legislation to be able to account for this kind of divergence and respond accordingly. The Cybercrimes Act has done so by including

the offence of cyber extortion. It recognises that all ransomware attacks are hacking crimes but that not all acts of hacking will amount to ransomware attacks. It was therefore important to require the specific intent to extort as an additional requirement of cyber extortion.

3.7.4 Section 11 of the Cybercrimes Act

Section 11 provides for aggravated offences. These, too, are ancillary offences which are operationalised via contraventions of sections 3(1), 5(1), 6(1), 7(1) and 10. In order for an offence under sections 3(1), 5(1), 6(1) and 7(1) to be considered an aggravated offence, it must be committed against a restricted computer system. A restricted computer system is defined in section 11(1)(b) as:

> any data, computer programme, computer data storage medium or computer system under the control of or exclusively used by—
> (i) any financial institution;
> (ii) an organ of state as set out in section 239 of the Constitution of the Republic of South Africa, 1996, including a court.

In this case, the suitable target is what differentiates an ordinary offence from an aggravated offence. For the aggravated offence derived from sections 5(1), 6(1) or 10, the consequences of the offence are an important consideration because they must cause considerable harm, such as endangering life, inflicting bodily injury or violating the physical integrity or physical freedom of any person or persons. They may cause also the destruction of or substantial damage to property (presumably, this includes incorporeal property); cause major economic loss; create serious public emergency situations; or prejudice the security, defence, law enforcement or international relations of the country.[144] Aggravated offences are so serious that section 11 provides that they may be prosecuted only on the written authorisation of the Director of Public Prosecutions.[145]

3.8 Summation

This chapter has introduced some of the social factors that allow for the successful commission of a cybercrime. The presence of a motivated offender is the first criterion in this regard. The internet provides a plethora of avenues for the motivated offender to

144 Section 11(2) of the Cybercrimes Act.
145 Section 11(3) of the Cybercrimes Act.

thrive. The hacker epitomises the motivated offender. She does this by employing many different techniques to attack the confidentiality, the integrity and the availability of the suitable target.

The nature of the internet constitutes fertile ground for deviancy. In the next chapter, the impact of the capabilities of the motivated offender will be unpacked. While the offences that have been discussed in this chapter qualify as true cybercrimes, those that are discussed in the next chapter do not meet the minimum requirements of being computer dependent and violating the CIA triad. This is a key point, for without these minimum requirements, although the motivated offender may identify a suitable target, the offence may be a Type II computer enabled crime, which ought to have no place in the Cybercrimes Act.

CHAPTER FOURTYPE II CYBERCRIMES: A SUITABLE TARGET

4.1 Introduction

In order to grapple with the issues surrounding Type II cybercrimes, it is necessary to take into consideration a philosophical matter termed the uniqueness debate. This debate deals with the moral and ethical questions related to ICT. Whereas full engagement with computer ethics debate is beyond the scope of this study, a brief engagement with the arguments will assist in evaluating whether there is sufficient uniqueness to support Type II crimes being considered as true cybercrimes. In other words, are Type II cybercrimes sufficiently different from terrestrial crimes or unique enough to warrant their elevation to true cybercrimes? This question is not peculiar to cybercrimes and it is not the first time that it has been raised, hence aspects of the computer ethics debate are discussed briefly below in order to provide some context and perspective to the issues raised in this chapter.

The traditionalists exist on one end of the spectrum, and on the other end are the philosophers who theorise the uniqueness of computer ethics. They are the proponents of the *Computer Ethics Is Unique* (CEIU) thesis. They do not hold a unified view about the uniqueness of computer ethics. Some argue that at least some aspects of computer ethics are unique, meaning that they did not exist before the advent of computing and ICT and, therefore, they raise *new* ethical issues. Other proponents of the CEIU School suggest that the uniqueness of computer ethics has been introduced by ICT, which brought with it certain moral problems which cannot be understood fully through our existing moral framework.[1] They submit that either there needs to be a new type of ethical theory or a whole new morality framework needs to be introduced.

Johnson states that the uniqueness issues are important because they are intertwined with a number of other important considerations, for instance, whether there is a need for the creation of a new field of study that will deal with computer-ethical issues. She observes that the computer revolution is neither the first nor the last technological advancement which will raise moral concerns. Take, for example, the concerns surrounding human cloning or the creation of the atom bomb or the development of nuclear capabilities.

1 Tavani (2002) at 38.

There are questions also of whether one should donate one's organs for transplant or whether employers should use drug tests to determine whether employees are using drugs or not.[2] More contemporary concerns have to do with the capabilities of drones in war zones or the fear of universal surveillance and privacy violations. These examples illustrate the fact that technological advancements, while beneficial in many cases, may not be good always. They tend to have mixed value, which means that they have to be evaluated morally as well as criminally, economically, environmentally and the like.[3]

For Type II cybercrimes, such as cyberstalking and online harassment, the conclusions are not black and white. This is so because they cannot be looked at purely from a legal or policy perspective; social and moral issues have to be taken into serious consideration also. The cyberbullying and "cyber sexploitation" case of Amanda Todd discussed in §4.3.1.1 below highlights some of these issues.

4.1.1 The Uniqueness View

When discussing the CEIU thesis, it is important to define what exactly is meant by the word "unique". The Merriam-Webster online dictionary defines it as (1) being the only one, (2) being without a like or equal or (3) unusual. Tavani notes that the Merriam-Webster definition is narrower than the commonly used definition of "unique", which refers to something which is "highly unusual" or "not very common or not typical".[4] He finds that it would not be necessary for something to be one of a kind to be considered unique but, by the same token, for something to be highly unusual will not suffice. He then proposes an addition to the meaning of unique which includes the requirement of novelty or newness. However, this requirement is not meant to say that anything which is novel or new automatically will qualify as unique. He adds that if *X* is to be classified as unique, it must be novel or new in a way that challenges: "(a) our existing schemes for categorisation and classification of that particular phenomenon; or (b) our existing modes of explaining and analysing *X*".[5] In other words, Tavani is advocating a notion of "novel or new" which will mean that for phenomenon *X* to be considered unique, *X* would have to require a new

2 Johnson (1999) at 2; See also Himma (2003) and Tavani (2010)
3 Johnshon (1999) at 2.
4 Tavani (2002) at 40.
5 Tavani (2002) at 40.

category, a new classification scheme, a new theory or even an entirely new foundational structure.[6]

4.1.2 The Traditionalist View

The traditionalist view holds that all that is necessary is to take the conventional ethical norms and principles and apply them to the new situations that may arise from computer and information technology.[7] The uniqueness debate then can address policy vacuums which exist. Say, for instance, there is a policy vacuum regarding the ownership of computer software: all that would be necessary to fill the vacuum would be for the lawyers, policy makers and judges to extend the existing property laws and apply them to the "new" thing.[8] The traditionalist view is said to be important on both a descriptive and normative level because not only does it describe how policy decisions are made, but it also gives recommendations about how policy vacuums should be filled. The traditionalist view enlists the idea that there is a tendency to draw upon the familiar social and moral ideas when developing policies and then to extend them to fit whatever new features are encountered in technology.[9]

On the normative level, the traditionalist view draws on past experiences to make sense of any new technological developments. For example, given that there are existing understandings of and expectations regarding the right to privacy or the right to freedom of speech in the terrestrial world, it becomes easier to understand what these rights would look like in cyberspace. Therefore, it makes sense that these experiences would be what one draws upon when filling policy vacuums.[10]

In Chapter One above, this study argued against the blind extension of existing laws and principles to cybercrime, because cybercrime possesses special characteristics which require individual adjudication to determine which principles apply and which do not. In this instance, the distinction between Type I and Type II cybercrimes has led to the conclusion that Type I cybercrimes are classified more appropriately as true cybercrimes because of

6 Tavani (2002) at 40. See also Tavani (2002, 2007 & 2010).
7 Johnson (1999) at 4, See also Johnson (1985, 1997, 2002, 2006 & 2008).
8 Johnson (1999) at 4.
9 Johnson (1999) at 4.
10 Johnson (1999) at 5.

their inherent features, whereas Type II cybercrimes are (in most cases) terrestrial crimes with a cyberspatial manifestation, which is not enough to classify them as true cybercrimes.

Bearing that in mind, it may be appropriate to apply the traditionalist view to determine how Type II cybercrimes ought to be dealt with when it comes to the filling of any policy vacuums. However, the traditionalist view, in some instances, may be too restrictive in its compass. Since it relies upon a mechanical process of applying existing norms to new situations, it may over-simplify the role and tasks of computer ethics.[11] Therefore, the CEIU thesis is important and instructive when deciding which approach to adopt for Type II cybercrimes.

4.2 Gordon & Ford Categorisation and the Routine Activities Theory

Chapter Two of this study identified the Gordon & Ford Categorisation (G&FC) as an important step in arranging cybercrimes into Type I and Type II groups. This chapter deals with cybercrimes which cannot be categorised legitimately as Type I but which may fall under Type II.

Type II cybercrimes have a more pronounced human element to them than Type I cybercrimes, which are more technical in nature.[12] They exist on the opposite end of the spectrum to Type I cybercrimes. They encompass a wide range of activities which may include cyberstalking and harassment, child predation, corporate and governmental espionage, and online terrorist activities.[13]

The first characteristic of Type II cybercrimes is that they are not facilitated by the use of crimeware — such as computer viruses, worms, bots, Trojans and spyware — which are instrumental in Type I cybercrimes. Instead, they are facilitated by ordinary computer programmes and tools, such as social media platforms, which are harmless unless they are "weaponised". Secondly, Type II cybercrimes generally consist of repeated activities in relation to their target. This means that the attack is not once-off or isolated when viewed from the perspective of the target.[14]

11 Johnson (1999) at 5.
12 Gordon & Ford (2006) at 13, Wadhwa & Arora (2017) at 2217.
13 Gordon & Ford (2006) at 14, Wadhwa & Arora (2017) at 2217.
14 Gordon & Ford (2006) at 15.

Gordon & Ford have stated that cybercrimes exist on a continuum, from crimes which are entirely technological in nature to those which are people-related at their core, although there are likely to be very few events which fit neatly under either Type I or Type II.[15] Be that as it may, their categorisation is essential to understanding cybercrime and acknowledging the range of activities that exists on this spectrum is important in the fight against cybercrime. In addition to the foundation which has been laid by Gordon & Ford, adoption of the minimum requirements set out in Chapter Two above will go a long way towards uncluttering the Cybercrimes Act and allowing it to be more effective. Said minimum requirements mean that, in order for an act to be considered a true cybercrime, it must be computer dependent and it must constitute an attack on the CIA triad. The only offences which meet these requirements are Type I cybercrimes and, therefore, only they ought to be included in the Cybercrimes Act.

Type II cybercrimes have become increasingly prevalent and, in many instances, they cause unimaginable emotional and financial distress to victims. Furthermore, because of their significant presence in cyberspace, their classification as cybercrimes is not questioned. In their discussion of Type II cybercrimes, Gordon & Ford describe the case of Amy Boyer who was murdered after she had been stalked online. The perpetrator is alleged to have used several online tools and websites to perpetrate the crime. They note that some analysts have questioned whether this and other similar crimes are genuine cybercrimes. However, they believe that such crimes are "by necessity a form of cybercrime, as the computing element fundamentally changes the scope of the crime", necessitating a Type II categorisation.[16] Still, they admit that the "cyber" element of the crimes committed against Amy Boyer was not pronounced enough to qualify them as true cybercrimes.

The position adopted in this chapter is that while Type II cybercrimes exist and cause great harm, they do not belong in the Cybercrimes Act because they are computer enabled. In essence, Type II cybercrimes enhance offline crimes which already have been addressed in existing common and statutory law. What is needed is for the existing laws to be amended to reflect the new cyberspace landscape and the troubles it brings.

15 Gordon & Ford (2006) at 15.
16 Gordon & Ford (2006) at 15.

Once offences have been categorised as either Type I or Type II cybercrimes, the Routine Activities Theory (RAT) comes into play. The kind of criminal activities with which RAT is concerned are predatory violations. These are illegal acts where someone definitely and intentionally harms the person of another or takes or damages the property of another.[17] Technically, RAT is confined to offences which involve direct physical contact between the offender and the target.[18] However, the theory was formulated in the 1970s and 1980s when the current capabilities of the internet were inconceivable. Today, direct predatory harm can occur without physical interactions. Compare, for example, the case of traditional bullying and cyberbullying. They are identical when one considers their essential elements and differ only in respect of physical contact which, when carefully considered, is an inconsequential difference.

The spatio-temporal character of RAT supports the view that physical contact is inconsequential to any kind of predatory violations. It will be recalled that the aetiological formula of RAT is:

crime = a motivated offender + suitable target – capable guardian

In simple terms, this formula requires the offender and the target to be present simultaneously at a "perpetration" location while the capable guardian is absent. For Type II cybercrimes, the locations may be the various platforms found in cyberspace, such as social networking platforms, which do not have a physical presence. Because of the instantaneous nature of these platforms and their constant interconnectedness, the offender and the victim may be on different continents physically, but interact as if they are in same room. For all intents and purposes, they will behave as if they occupy the same space at the same time, thus satisfying the requirement of spatio-temporal convergence. This is one of the defining characteristics of Type II cybercrimes which may differentiate them from their offline counterparts, but its effect is minimal.

4.3 Part II of Chapter 2 of the Cybercrimes Act: Malicious Communications

Part II of Chapter 2 of the Cybercrimes Act, titled "Malicious Communications", is reserved for Type II cybercrimes. All the crimes that were discussed in the previous chapter of this

17 Glaser (1974) at 4.
18 Cohen & Felson (1980) at 390.

dissertation met the minimum requirements to be classified as Type I cybercrimes, except the crime of cyberfraud which is contained in Part II of Chapter 2 of the Cybercrimes Act but is classified — incorrectly — as a Type I cybercrime. Cyberfraud will be discussed with the Type II cybercrimes and the reasons for this will become clear later.

Part II of Chapter 2 of the Cybercrimes Act is aimed at criminalising the dissemination of harmful data messages. Its key provisions are to be found in sections 14, 15 and 16. Section 14 criminalises making available, broadcasting or distributing data messages which incite damage to property belonging to, or violence against, a person or a group of persons.[19] Section 15 outlaws making available, broadcasting or distributing data messages which threaten persons with damage to property or violence. Section 16 criminalises the transmission of data messages that are intimate in nature, as when nude images of a person are distributed without the consent of the person.[20]

By way of an executive summary of the ensuing discussion, the argument is that all four crimes considered ought not to be in the Cybercrimes Act. The crime in section 14 does not possess a significant enough cyber presence to be categorised even as a Type II cybercrime.[21] The crimes in sections 15 and 16 do possess significant enough cyber-related characteristics to be classifiable as Type II cybercrimes but they, too, should not be in the Cybercrimes Act. The reason for this is that they are not true cybercrimes, in the sense that they are not computer dependent and they do not trespass against the CIA triad. Furthermore, all of these crimes (regardless of whether they are classifiable as Type II cybercrimes or not) may be dealt with adequately under the existing common law, as they are merely online manifestations of existing offline offences. All that is needed is for existing laws to be amended or interpreted to acknowledge the role of cyberspace where necessary. Therefore, arguing that these offences are not true cybercrimes is not an attempt to avoid addressing them; rather, it is an attempt to unburden the Cybercrimes Act in order to ensure that it is effective when enacted.

19 This offence will be discussed along with cyberfraud contained in section 8 of the Cybercrimes Act.

20 [B6—2017], Explanatory Notes at 68. Apart from some minor differences of word choice between versions [B6—2017] and [B 6B—2017] of the Cybercrimes Bill and as such the Cybercrimes Act, these provisions are substantively the same, and the Explanatory Notes to [B6—2017] are quite instructive.

21 The same applies to the crime of cyberfraud provided for in section 8. See §4.3.3 below.

4.3.1 Section 15 and Section 16 of the Cybercrimes Act

This part will consider Type II cybercrimes from the perspective of the suitable target. The suitable target offers an interesting angle because a human target brings a dimension to the crime that an inanimate object, like a computer system, does not. One of the hypotheses meant to be tested by RAT is how the suitability of the target influences predatory contact. In determining the suitability of a target, the four constitutive properties designated by the acronym VIVA (value—inertia—visibility—access) are indispensable.

The value of a target refers to the victim's desirability to the offender. If one considers the offences relating to online harassment, the type of harassment perpetrated will depend on what the offender hopes to gain from the victim. It may be a desire to cause emotional distress to the victim in the case of cyberbullying; a desire for revenge against an ex-lover in the case of non-consensual pornography; or the pursuit of sexual gratification for a child pornographer.

Inertia, in its original pronouncement, referred to the physical properties of the target. It speaks to the mobility of the target where the question, in the case of personal violations, is whether the victim is able to resist predation. Here, the constant connectedness that the internet brings plays the biggest role in the victim's inability so to resist.

Visibility relates to the idea that targets who are prominently visible to the offender are more likely to be chosen than those who are not. Like inertia, the constant interconnectedness of the internet is a major contributing factor to the visibility of the target.

Finally, accessibility refers to the ease with which an offender is able to gain legal or illegal access to the target for purposes of committing a violation. It also refers to the opportunities available for non-detection and escape. Here, the opportunities to escape are more pronounced because of the offender's ability to be anonymous and pseudonymous on the internet.

4.3.1.1 Section 15: Data Message which Threatens Persons with Damage to Property or Violence

Section 15 of the Cybercrimes Act provides that:

> A person commits an offence if he or she unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message which—
> (a) threatens a person with—
> (i) damage to property belonging to, or violence against, that person; or
> (ii) damage to property belonging to, or violence against a related person; or
> (b) threatens—
> (i) a group of persons;
> (ii) any person forming part of that group of persons; or
> (iii) any person associated with that group of persons,
> with damage to property belonging to, or violence against—
> (aa) that group of persons;
> (bb) any person who forms part of that group of persons; or
> (cc) any person who is associated with that group of persons,
> and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message, either by itself or in conjunction with any other data message, as a threat of damage to property or violence to a person or category of persons contemplated in paragraph (a) or (b), respectively.

Section 15 criminalises the unlawful and intentional making available, broadcast or distribution, by means of a computer system, of a harmful data message. The elements of unlawfulness and intention have been discussed before and need no further explanation; and the content of making available, broadcasting and distributing data messages may be understood in their ordinary meaning.

A data message is harmful when it threatens a person with violence or damage to her property; or threatens to harm similarly one related to said person. It is harmful also when it threatens a group of persons, a member of said group, or anybody associated with said group with violence or damage to property belonging to that group or person. In addition, the data message in both scenarios ought to be regarded as a threat — to the designated property or person(s) — by a reasonable person "in possession of the same information and with regard to all the circumstances".

In terms of section 15, there are two types of suitable targets. The first is a specific individual and everything associated with her, such as her property and her family, or those with whom she has a close relationship, and their property. The second is a group of people or an individual who is identifiable as being a part of that group. The composition of the

group in question has not been specified by the Cybercrimes Act, but it may be assumed that it refers to groups constituted along racial, social, cultural, political or religious lines, to name a few.

The VIVA value of the suitable target will depend upon the proclivities of the motivated offender, which means it will vary from one offender to another. One of the reasons for this is that with Type II cybercrimes, financial gain is not the obvious motivation for the offender, as is apparent in Type I cybercrimes. If, for example, an offender is a cyberbully, she would find an individual with a fragile mental constitution to victimise. Section 15 of the Cybercrimes Act would apply to the case where the cyberbully distributes on social media data messages which threaten a victim with some form of violence in order to cause her mental or psychological harm. In that case, a teenage girl may be more valuable as a target than a middle-aged man who does not engage regularly on social networking platforms. Similarly, as far as groups are concerned, if the motivated offender were looking for some kind of economic gain for herself or economic loss for her target, she could spread false information about a big corporation, which may be more successful than an attack upon a small community organisation. As far as violence goes, the Cybercrimes Act does not limit it to physical violence, but leaves it open-ended. In section 15, one is dealing with the *threat* of violence which means that one must take into account the emotional and psychological toll of such threats. Cyberbullying and cyber sex exploitation or sextortion, as discussed below, are apt examples.

The VIVA inertia of a suitable target refers to the target's ability to resist the violation directed at her. Take, for example, a threat of violence directed at an individual and her property. A wealthy person with the means to hire private security to protect herself is likely to resist successfully threats which are designed to instil fear in her. Furthermore, she would have the means — the money, power and status — to elicit the help of law enforcement and the courts to track down the offender or force him to desist in his harassment of her.

The internet plays a significant role as regards VIVA visibility. A target may expose herself unintentionally to victimisation by the way in which she conducts herself on the internet. For example, in order to use the internet, one is expected to have multiple online profiles which usually are interconnected. It is expected also that the user provide

information which may appear trivial but actually may be helpful to a cyberstalker or a cyberbully. An offender may be able to gain personal identifying information about the target — such as where she lives, works, socialises and the people with whom she is in contact — making it difficult for the victim to escape online harassment by the offender.[22]

This is illustrated best by the tragic case of Amanda Todd, an 11-year-old girl from British Columbia in Canada, who was coaxed into exposing her breasts to strangers over a BlogTV live webcam session.[23] Unbeknownst to her, one of the users took a screenshot of Amanda with her breasts exposed and used it to blackmail, harass and sexually extort her. When Amanda's topless picture was posted online, she became a victim of "slut-shaming", which is a term used to describe "the shaming [or harassment] of a girl because she has casual sex or is perceived to have casual sex".[24] Although slut-shaming is not new, it has gained a lot of traction in recent years, with the growth and popularity of social media — and it is prevalent in the experiences of victims of revenge porn, cyberbullying and online harassment. Tragically, the story ends with young Amanda committing suicide following four years of harassment by her tormenters.[25]

It is reported that the motivated offender in this case, identified as a Mr Corban, used upwards of 90 screen names on social media platforms to target more than 75 victims from around the world. Much of the stalking and "sextortion" (sexual extortion)[26] of Amanda Todd was carried out via Facebook and, after her untimely suicide (which sparked an international public outcry), Facebook compiled a report which it handed over to the police and which eventually led to the arrest of Corban. The Canadian Police also opened investigations into 10 potential victims of Corban, including Amanda Todd.[27]

VIVA accessibility is aided largely by the fact that the internet cannot be shut down. One of the challenges with cyberbullying,[28] when compared to offline bullying, is that in the

22 Martellozzo (2017) at 109.
23 White (2014) at 1.
24 Messit (2014) at 51.
25 CBS News (2013) at 1.
26 Sextortion is an emerging criminal practice where a perpetrator may gain access to intimate or compromising footage of a target with the aim of blackmailing her into performing further sexually related acts, thereby entrapping her further. Jane & Martellozzo (2017) at 9.
27 Subramaniam & Whalen (2014) at 1.
28 Brickwell defines cyberbullying as "the repeated use of communication technologies – texts, instant messages, and social networking sites – to harass or socially exclude others. It may include the

latter case the victim may be able to escape her bullies at school when she goes home. With cyberbullying, however, unless she is able to disconnect completely from the internet, she has no avenues of escape. Furthermore, accessibility also speaks to the ease with which the offender can escape and avoid detection. The internet presents innumerable opportunities to avoid detection because of the means it provides to be anonymous or pseudonymous.[29]

Amanda Todd's story is tragic but it is not unique.[30] She endured most of the harm that is envisioned in section 15 of the Cybercrimes Act. It is not uncommon, in the case of cyberstalking, cyberbullying and online harassment, for the motivated offender continuously to victimise his target. The fact that Amanda Todd was 11 years old made her a particularly suitable target to Corban because her age added to her value. It meant that she was easier to manipulate and control than if she had been 30 years old. Corban threatened her with violence as he communicated with her via social media in an attempt to coerce her into sending more nude photographs of herself. When she did not succumb to his demands, he posted her pictures on Facebook and ensured that they could be viewed by her school mates and her family members. This led to secondary victimisation of Amanda by her peers as persistent cyberbullying followed her, even when she moved to another town and a different school. She endured harmful data messages which mocked her and encouraged her to self-harm by taunting her to kill herself. In addition, as intimated above, there were false rumours spread about her, which resulted in a "slut-shaming" campaign against her. All that culminated in her untimely demise.[31]

Most of the harassment of Amanda Todd was conducted over the internet, meaning that it had a significant enough cyberspace presence to warrant its classification as a Type II cybercrime. However, there remain the minimum requirements[32] which are not met and hence disqualify harmful data messages as true cybercrimes. Existing laws, such as those that deal with defamation and sexual offences, could address adequately situations such as these if they are amended to reflect the advancements in technology and the internet.

---

distribution of unsolicited and unwanted 'text or photos of a sexual nature or requesting sexual acts either online or offline." Brickwell (2017) at 49.

29 Hickle (2017) at 99.

30 See discussion of the 2016 report from the Brookings think tank which analysed 78 sextortion cases in Wittes et al. (2016) at 2-6.

31 CBS News (2013) at 1.

32 These are computer-dependent cybercrimes which are an attack on the CIA triad.

For example, the law of defamation could address situations such as Amanda's. Defamation consists of the unlawful and intentional publication of matter concerning a person which tends to injure that person's reputation. Reputation may be differentiated from dignity, in that reputation is concerned with the esteem in which the victim is held by society, whereas dignity refers to how she views herself. It is not enough for a case of defamation that only the victim's dignity is impaired.[33] There are four essential elements of defamation, namely, (1) intention, (2) unlawfulness, (3) publication and (4) defamatory matter referring to another. Intention and unlawfulness are non-contentious and need no further discussion. The third element requires that the publication be made to someone other than the complainant.[34] The manner in which the publication is made will not make a material difference, therefore defamatory material published via the internet is covered by this offence. The material published must be defamatory. It is understood that defamatory material may take various forms, ranging across words, written or spoken, acts or even omissions. Defamatory material is defined as material which exposes the victim to hatred, ridicule or contempt or which diminishes her reputation.[35]

Further, the Protection from Harassment Act 17 of 2011[36] is a piece of legislation which would address adequately issues of online harassment if it is amended to account for offences occurring online. It offers protection for persons who are harassed in ways which cause mental, emotional and economic harm to the victim.[37] The Act also affords the complainant the opportunity to seek a protection order from the Magistrates' Court.[38]

4.3.1.2 Section 16: Distribution of Data Message of Intimate Image

Section 16 of the Cybercrimes Act reads:

> (1) Any person ("A") who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of a person ("B") without the consent of B, is guilty of an offence.
>
> (2) For purposes of subsection (1)—
>
> (a) "B" means—

33 Burchell (2016) at 643.
34 Burchell (2016) at 643.
35 Burchell (2016) at 644.
36 Act 17 of 2011.
37 See section 1 of the Protection from Harassment Act.
38 Section 2 of the Protection from Harassment Act.

(i) the person who can be identified as being displayed in the data message;
(ii) any person who is described as being displayed in the data message, irrespective of the fact that he or she cannot be identified as being displayed in the data message; or
(iii) any person who can be identified from other information as being displayed in the data message; and

(b) ''intimate image'' means a depiction of a person—
(i) real or simulated and made by any means in which—
(aa) B is nude, or his or her genital organs or anal region, or if B is a female, her breasts, are displayed; or
(bb) the covered genital or anal region of B, or if B is a female, her covered breasts, are displayed in a manner that violates or offends the sexual integrity or dignity of B; and
(ii) in respect of which B so displayed retains a reasonable expectation of privacy at the time that the data message was made.

Section 16 addresses the crime of non-consensual pornography, otherwise known as revenge porn. It makes it an offence intentionally and unlawfully to distribute a data message of an intimate image without consent.

Non-consensual pornography involves the uploading of photos or videos (typically of a nude or sexual nature) of a person onto the internet without the subject's consent. In the instances where this is done by a former lover with the intention of humiliating and harassing the victim as an act of vengeance, it may be termed revenge porn.[39] The latter is a subset of the broader problem of non-consensual pornography. In this discussion, both revenge porn and non-consensual pornography will be used to describe the various scenarios that may arise.[40]

Non-consensual pornography or revenge porn encompasses a range of behaviours, which may include the production or distribution of sexually explicit images of a person without his or her consent. These explicit materials may be obtained in a number of ways, for example, by hacking into the victim's computer system and stealing naked images, or by surreptitiously recording or taking pictures of the subject engaged in intimate activities. In another scenario, the victim may give intimate pictures to the offender or give consent to being filmed by her, perhaps in the context of a romantic relationship, with the (sometimes

39 Poole (2015) at 184; Jane (2017) at 69.
40 Poole (2015) at 184.

implicit) understanding that the materials are to remain private.[41] The offender then would post the images or videos onto the internet, either on a revenge porn site or on social networking sites, like Facebook and Twitter, with the aim of harassing the subject or extorting her.[42] Revenge porn displays some of the potentially negative consequences of "sexting", a common activity, particularly amongst the youth, which involves the sharing of sexually suggestive photographs, videos or messages with someone else via text.[43]

IsAnyoneUp.com was a revenge porn site run by Hunter Moore which, like some other revenge porn sites, encouraged the users of the site to supply the victim's personal information so that she could be identifiable to other users.[44] This practice was encouraged actively, by prompting the uploader to provide the subject's full name, city of residence, profession and links to her social network profiles.[45] This meant that the pictures and videos would be linked to the victim's online profile, which resulted in their being accessible via a simple Google search of the victim's name. This additional component gave the site its popularity and led to victims being stigmatised and ostracised.[46] This practice is referred to as doxxing.[47]

Revenge porn poses serious risks of offline stalking and physical harm. In a study involving 1 244 individuals, it was found that over 50% of the victims reported that their names and social network profiles had appeared next to the naked pictures.[48]
Twenty per cent of the victims reported that their telephone numbers and email addresses also had appeared next to their naked photographs.[49] Publication of this private information almost certainly encourages consumers of revenge porn to approach the victims and harass them further. Revenge porn also has serious psychological consequences for victims.[50] According to the Cyber Civil Rights Initiative, more than 80% of revenge porn victims have

41 Poole (2015) at 185.
42 Temple (2013) at 1, Jane (2017) at 69
43 Calvert (2015) at 678; Jane (2017) at 69.
44 Morris (2012) at 1.
45 Morris (2012) at 1.
46 Morris (2012) at 1.
47 Jane (2017) at 69.
48 Citron & Franks (2014) at 105.
49 Citron & Franks (2014) at 105.
50 Jane (2017) at 69-70.

reported experiencing severe emotional distress and anxiety.[51] Some women have reported being afraid of leaving their homes for fear that someone might act upon threats posted online or made via phone calls.[52] Also, revenge porn may be used as a form of domestic abuse,[53] where the dominant party in the relationship coerces the weaker partner into taking sexually explicit pictures as a form of control. In other cases, the materials may be used as a form of blackmail to prevent the victim from leaving the relationship by the perpetrator threatening to disclose said materials. Other circumstances have revealed that victims can lose their jobs or struggle to find employment because a simple Google search of their names reveals the explicit photographs.[54]

When the Cybercrimes Act first was presented for public comment in 2015, it did not have a provision addressing non-consensual pornography. Version [B6—2017] addresses non-consensual pornography in section 18, the content of which is replicated in section 16 the Cybercrimes Act.

One of the elements of this offence is that the image should be of an identifiable person. Section 16 does not stipulate which features of the person would qualify as identifying features. It may be argued, therefore, that the features in question do not have to include the person's face necessarily, but can be other identification markers, such as a prominent and unique tattoo. The provision further requires that the designated images have to be "intimate images" which are defined as images which can either be real or simulated where the subject is nude or his or her genital organs, anal region or breasts are displayed. Where those areas are covered then they are intimate images when they are displayed in a manner that violates or offends the subject's integrity or dignity. Furthermore, intimate images are depictions in respect of which the subject so displayed retains a reasonable expectation of privacy at the time that they were made. This means that a person who poses naked for an online pornographic magazine is deemed to have given consent to the pictures being distributed and therefore cannot claim a reasonable expectation for privacy.

51 Citron & Franks (2014) at 106
52 Citron & Franks (2014) at 104.
53 Martellozzo (2017) at 7.
54 Citron & Franks (2014) at 104, Martellozzo (2017) at 12 – 13; Jane (2017) at 69.

As regards non-consensual pornography, the Cybercrimes Act builds upon and makes amendments to the Sexual Offences and Related Matters Amendment Act (Sexual Offences Act) of 2007. The Schedule to the Cybercrimes Act inserts section 10A into the Sexual Offences Act. This section deals with the harmful disclosure of pornography and stipulates, *inter alia,* that:

> (1) A person (‘‘A’’) who unlawfully and intentionally discloses or causes the disclosure of pornography in which a person 18 years or older (‘‘B’’) appears or is described and such disclosure—
> (a) takes place without the consent of B; and
> (b) causes any harm, including mental, psychological, physical, social or economic harm, to B or any member of the family of B or any other person in a close relationship to B, is guilty of the offence of harmful disclosure of pornography.
>
> (2) A person (''A'') who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1) and such threat causes, or such disclosure could reasonably be expected to cause, any harm referred to in subsection (1)(b), is guilty of the offence of threatening to disclose pornography that will cause harm.
>
> (3) A person (''A'') who unlawfully and intentionally threatens to disclose or threatens to cause the disclosure of pornography referred to in subsection (1), for the purposes of obtaining any advantage from B or any member of the family of B or any other person in a close relationship to B, is guilty of the offence of harmful disclosure of pornography related extortion.

This addition to the Sexual Offences Act places the prohibition upon non-consensual pornography in the same category as other sexual offences. It ensures that this offence is taken as seriously as other sexual offences and not left to the obscure fringes of cyberspace and cyber law.

The Cybercrimes Act takes matters further by making the courts available to victims when there is a need for recourse. It inserts section 10A(4)(a) into the Sexual Offences Act, which provides that any person who lays a charge of non-consensual pornography with the police, may apply *ex parte* to the Magistrates’ Court for an order to prohibit the disclosure of the offending pornographic material or to order the removal of or blocking of access to said materials by an internet service provider or any person controlling a computer system. What this amendment does is to provide immediate relief to the complainant.

Given that the application is *ex parte*, the complainant does not have to be at the mercy of the offenders. Furthermore, section 10A(4) of the Sexual Offences Act does not impose criminal or civil liability upon the persons, natural or juristic, who have disclosed or

intend to disclose the pornographic material. Hence, it would be relatively easy for them to comply with the court order. Of course, should they feel that their rights are being infringed — for example, their right to freedom of speech — then they can approach the court to challenge the order. Should they not comply with a valid court order, then they would be liable to be charged with contempt of court. Section 10A(4) of the Sexual Offences Act will go a long way to protecting the interests of the victims of non-consensual pornography.

Compared to, say, the Communications Decency Act (CDA) of 2012 in the United States, the Cybercrimes Act is rather progressive with this amendment. Section 230 of the CDA says that:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

This provision gives immunity to internet service providers and a range of interactive computer service providers for any content uploaded or published by third parties. Hence, they cannot be held liable for said content.[55] This immunity also means that even if the content were uploaded by an individual who obtained it illegally by means of hacking, there is no obligation on the internet service provider to remove it upon request from the victims.[56] The same is true where the offender came into possession of the content legally but had no permission to post it. Internet service providers are distinguished from information content providers, which are defined as persons or entities that are "responsible, in whole or in part, for the creation or development of information provided through the internet".[57] Information content providers do not enjoy the immunity afforded to internet service providers.

Protection provided by the courts is important because in cases where the victim had to approach the offender or the owners of the revenge porn site directly, they made themselves vulnerable to extortion and further victimisation. The revenge porn site called *UGotPosted.com*, allegedly run by one Kevin Bollaert, included personal identifying information of the victims and links to their social networking pages.[58] However, Bollaert

55 Goodin (2014) at 1.
56 Poole (2015) at 197.
57 Section 230(f)(1) of the Communications Decency Act, 2012.
58 Walker (2013) at 1.

took it a step further than others by creating a second website called *changemyreputation.com* which he used to contact the victims and inform them that their pictures had been posted on a revenge porn site. He would then offer to remove the pictures for a fee of $300—$350. In a year between 2012 and 2013, there were more than 10 000 pictures posted on *UGotPosted.com* and about 2 000 emails requesting that the pictures be removed. Many of the victims paid the removal fee, earning Bollaert thousands of dollars.[59] In December 2013, he was arrested by California Department of Justice agents, who charged him with thirty-one counts of identity theft, extortion and conspiracy.[60]

4.3.2 Section 14: Data Message which Incites Damage or Violence

Section 14 of the Cybercrimes Act provides that:

> Any person who unlawfully makes available, broadcasts or distributes, by means of a computer system, a data message to a specific person, group of persons or the general public with the intention to incite—
> (a) the causing of any damage to any property belonging to; or
> (b) violence against,
> a person or a group of persons, is guilty of an offence.

This section renders it an offence to make available, broadcast or distribute a data message which may incite harm. It prescribes the medium through which the data message may be made available, broadcasted or distributed, namely, a computer system. It also specifies to whom the data message should be directed, that is, a specific person, a group of persons or the general public. Finally, it prescribes the intention that must accompany the action, which is to incite violence against a person or a group of persons, or to cause damage to any property belonging to a person or a group of persons.

The crime created by section 14 is comparable to the common law inchoate crime of incitement, which also has been legislated in the Riotous Assemblies Act.[61] Section 18(2)(b) of the Riotous Assemblies Act provides that it is an offence to incite, instigate, command or procure a person to commit any common-law or statutory offence. The person who incites (the inciter) is defined as "one who unlawfully makes a communication to another with the intention of influencing him or her to commit a crime".[62] The one who is incited to commit

59 Poole (2015) at 183.
60 Jane & Martellozzo (2017) at 11 – 12.
61 Riotous Assemblies Act 17 of 1956.
62 Burchell (2016) at 537; *Nkosiyana* 1966 at 658H.

an offence is known as the incitee. The inciter is liable, upon conviction, to the punishment which would have been imposed upon a person convicted of actually committing the offence in question.

The existence of section 18(2)(b) of the Riotous Assemblies Act begs the question of whether section 14 of the Cybercrimes Act is a necessary or even useful provision. Section 14 of the Cybercrimes Act and section 18(2)(b) of the Riotous Assemblies Act are alike in their core aspects. The essential elements in section 14 are (a) unlawfully; (b) making available, broadcasting or distributing data messages; (c) with the intention to incite damage to a person's property or violence against a person or group. The unlawfulness element in both provisions revolves around a communication made by the inciter to the incitee. The Riotous Assemblies Act does not prescribe the manner in which the communication must be made, whereas the Cybercrimes Act does. The Riotous Assemblies Act is interpreted to mean that the communication can be made verbally or by conduct, but it is accepted also that it can be made via a wholly automated computer system.[63] The Cybercrimes Act specifies that the data message must be communicated "by means of a computer system". In particular, section 14 stipulates the unlawful conduct as that which makes available, broadcasts or distributes the data message, which means that the motivated offender need not necessarily be the author of the inflammatory data message, but can be the vessel through which it is sent. For example, if an online magazine publishes an article which incites violence, the editors of the magazine may be held liable criminally if they possess the necessary intention to incite.

This approach is supported, in the context of offline incitement, by so-called chain incitement.[64] Snyman describes chain incitement as incitement to incite. He gives the illustration of a woman inciting her son to hire a hitman who will kill her husband. The number of links in the incitement chain does not absolve the woman from liability for incitement. By the same token, if Amu emails an inflammatory data message to Basani for her to post on her social media platform that would incite Cassandra to commit an act of harm against a person, both Amu and Basani would be guilty of inciting Cassandra. However, when a computer programme, such as a social networking platform, is used, it

63 Burchell (2016) at 537.
64 Snyman (2008) at 303.

may prove problematic should the inciter broadcast a data message indiscriminately onto the internet, without identifying a specific incitee. The question then becomes: does this qualify as a case of attempted incitement, a case of failed incitement or is it not incitement at all? This question was dealt with in *R v Segale*,[65] in which the appeal court upheld a conviction of incitement where the people who were incited to commit a crime were not particular persons or a particular group of persons, but rather "the whole of the non-European labour force of the Witwatersrand".[66] Therefore, although the communication must reach the mind of the incitee, it is not necessary for the inciter to know the identity of the person or persons incited. Furthermore, it is immaterial whether the incitee acts upon the communication or not, since no causal relationship between the incitement and the commission of the offence is required.[67] Where the inflammatory communication does not reach the mind of the incitee, then it may be counted as attempted incitement, for example, if Amu's inflammatory email ends up in Basani's spam folder and is never read by Basani.[68] All in all, it is fair to say that all the conduct elements of section 14 of the Cybercrimes Act are dealt with adequately under the common law and the statutory crime of incitement.

The second essential element is intention, which entails that the inciter must have intended the communication to reach the incitee. In other words, the inciter must know or, at least, foresee the possibility that the communication would reach the mind of the incitee.[69] Incitement cannot be committed negligently.[70] There is no indication that the intention element in section 14 of the Cybercrimes Act should be understood differently from that in section 18 of the Riotous Assemblies Act.

In essence, section 14 of the Cybercrimes Act and section 18 of the Riotous Assemblies Act provide for the same offence, but for the medium through which the incitement is committed. If necessary, this can be remedied by amending the Act to acknowledge online incitement. The offence provided for in section 14 of the Act is neither computer dependent nor an attack upon the CIA triad, and hence cannot be classified as a true cybercrime. Whether or not this offence may be categorised even as a Type II

65 *Segale* 1960 (1) SA 721 (A).
66 *Segale* 1960 at 731A.
67 Snyman (2008) at 299.
68 See *Nkosiyana* 1966 (4) SA (A) at 659.
69 Burchell (2016) at 533.
70 Snyman (2008) at 301.

cybercrime would probably have to be determined on a case-by-case basis, depending on how significant the online presence is.

4.3.3 Section 8: Cyberfraud

The crime of cyberfraud is an anomaly in the Cybercrimes Act. It is contained in section 8 of Part I of Chapter 2 of the Act. Presumably, the drafters of the Act considered cyberfraud to be a true cybercrime which could subsumed under Type I cybercrimes. This is incorrect. Not only is cyberfraud not a true Type I cybercrime, but it also does not qualify even to be considered a Type II cybercrime because it lacks sufficient cyber-related characteristics.

Cyberfraud is considered to be a major concern in South Africa,[71] which concern resulted in the inclusion of section 8 of the Cybercrimes Act. Unfortunately, the explanatory notes to the Bill [B6 B -2017] do not give any significant insight into the reasoning behind the creation of a new crime of cyberfraud when an expansive crime of common-law fraud already exists. The notes simply state that the Act—

> aims to create the statutory offence of cyber fraud by specifically criminalising fraud by means of data or a computer programme, or through the interference with data or a computer programme.[72]

While this declaration might appear compelling at first glance, in reality it is not.

It is submitted that certain offences commonly accepted as cyber fraudulent do not qualify as true cybercrimes because they do not meet the minimum requirements that would elevate them from ordinary offline fraud offences to cyberfraud. Further, in order for a fraudulent act to be transformed from offline fraud into cyberfraud, it needs to be a computer dependent act rather than merely a computer enabled act. Therefore, there is no need for section 8 in the Cybercrimes Act because the common-law crime of fraud is capable of addressing computer enabled fraud adequately.

Section 8 provides that:

> Any person who unlawfully and with the intention to defraud, makes a misrepresentation—
>
> (a) by means of data or a computer programme; or
> (b) through any interference with data or a computer programme as contemplated in subsection 5(2)(a), (b) or (e) or interference with a

71 Kilian (2017) at 1.
72 Cybercrimes and Cybersecurity Bill Explanatory notes (B6 – 2017) at 67.

> computer data storage medium or a computer system as contemplated in section 6(2)(a), which—
> (i) causes actual prejudice; or
> (ii) is potentially prejudicial,
> to another person is guilty of the offence of cyberfraud.

This definition may be compared to the common-law definition of fraud, which provides that fraud is the unlawful and intentional making of a misrepresentation which causes actual or potential prejudice to another.[73]

The essential elements of cyberfraud and common-law fraud are identical. They are (1) unlawfulness; (2) intention; (3) misrepresentation; and (4) prejudice. The Cybercrimes Act does not indicate that these elements must be interpreted differently from the elements of ordinary fraud, and it therefore is unnecessary to delve into the details of all the elements. The exception is the element of misrepresentation. While common-law fraud does not specify the manner in which the fraudulent act must occur, the Cybercrimes Act does. As is apparent from section 8(a) & (b), the misrepresentation must be performed by means of data or a computer programme, or through any interference with data or a computer programme (as per section 5(2)), or through interference with a computer storage medium or computer system (as per section 6(2)).

Misrepresentation sometimes is expressed as a "perversion or distortion of the truth".[74] It means that A must represent to B as true a condition or a set of conditions which is not actually true. In the common law, the manner in which a misrepresentation occurs does not matter. In some cases it may take the form of spoken or written words, but it also may be expressed in conduct, such as a nod of the head signifying consent.[75] The idea is well-established that a misrepresentation can take any form which is deceiving and misleading. This means that when there are technological advancements which allow for new forms of misrepresentation, such forms may be considered to resort under the common-law definition of fraud. In other words, new forms of misrepresentation do not add to or remove anything from the accepted elements of fraud. In turn, this means that the creation of a new crime of cyberfraud is unnecessary.

---

73 This definition was confirmed in *Myeza* 1985 (4) SA 30 (T) at 31-32, in *Ex parte Lebowa Development Corporation Ltd* 1989 (3) SA 71 (T) at 101 and in *Gardner* 2011 (1) SACR 570 (SCA) para 29.

74 Snyman (2014) at 524.

75 Snyman (2014) at 524.

Notwithstanding its complete concordance with common-law fraud, cyberfraud has been discussed as if it is deserving of being considered a new and stand-alone offence. For that reason, it is necessary to consider some of the popular views about cyberfraud. One of the first steps in determining whether an offence may be classified rightly as a cybercrime is to determine whether it is a computer dependent offence or a computer enabled offence.

Crimes known today as computer enabled crimes are actually those crimes which, for the most part, pre-date the existence of computers, the internet and cyberspace. In other words, computer enabled crimes are pre-existing terrestrial crimes committed with the help of computers.[76] These are crimes such as fraud, pornography, money laundering and (sexual) harassment. By contrast, computer dependent crimes are the crimes that are inseparable from the development of computers, the internet and cyberspace. They are the crimes which emerged in tandem with the internet and cannot exist without it, such as hacking and malware attacks.[77] The difference between computer enabled and computer dependent cybercrimes rests on the role that technology plays in the commission of the crime, specifically on whether or not it would have been possible to commit the crime without reliance upon a computer.

Examples of offences which commonly are referred to as cyberfraud are discussed below. In order to determine whether they are true cases of cyberfraud, they must be classified as either computer enabled or computer dependent. If they are computer dependent offences and cannot be dealt with adequately under the common-law definition of fraud, then they may be raised to the status of cybercrimes.

4.3.3.1 Fraudulent Online Sales

Online shopping has become a very popular form of shopping because it is very convenient and cost effective. Many stores offer online sales services which are secure and reliable, adding to the popularity of online shopping. The internet has made it possible also for individuals to transact with one another directly on platforms such as *eBay* and *Gumtree.*

Critics have asserted that although these transactions are beneficial to individuals who wish to sell and buy goods, they can be problematic in that they present a risk to both

76 Sallavaci (2016) at 54.
77 Maimon & Louderback (2019) at 192.

the seller and the buyer. For example, a seller may not wish to release the goods or services until payment has been secured and the buyer may not want to make payment before the goods or services have been delivered.[78] This makes it difficult, because neither party has any guarantee that the transaction will be completed in accordance with the agreed terms and conditions.

There are certain instances where a seller may advertise a product which does not exist or is one which is considerably different from that which was advertised. In other instances, a buyer may pay for the product via a debit order which she later reverses or cancels after the seller has delivered the product. And because these are private transactions between private individuals, there usually are limited avenues for recourse outside of claims under contract law. Another manifestation of this type of scam is the advertising of non-existent rental properties online. In these cases, victims may be asked to send the offender information which ordinarily would be confidential, such as bank statements with personal identifying information, supposedly to confirm that the target can afford the rent. Such information is very valuable to a person intending to commit identity theft. In other cases, a victim may be requested to pay the deposit for a rental property which does not exist or is not actually available for renting.[79] The reliance upon the internet in these cases means that the victim is disadvantaged by being deprived of the visual and social clues that would guard against the fraud. The anonymity that is provided by the internet also makes apprehending the offender difficult, if not impossible.

Be that as it may, the perpetration of this crime is by no means computer dependent. It is merely computer enabled. Indeed the internet has provided a platform for this fraud to be committed on a larger scale,[80] by providing the offender with access to more suitable targets. Although it may have been more tedious and time-consuming to do so offline, the same fraud could have been committed by word of mouth, by newspaper advertisements or by posting flyers on a street lamp. It is not enough to assert that, because the transaction was completed via an online platform, it is a cybercrime. It would be possible to find the offender guilty under the common law of fraud. The existence of the

78 Clough (2015) at 211.
79 Cross, Smith & Richards (2014) at 2.
80 Sallavaci (2017) at 54.

internet makes commission of the crime more efficient, but that is ultimately a secondary consideration. Expedience cannot create a new crime.

4.3.3.2 Advance Fee Fraud

The advance fee scheme has become one of the more common forms of online fraud. This type of fraud includes lottery fraud, romance scams and inheritance schemes. The methods by which it is perpetrated may differ, but the common factor is a promise of a reciprocated benefit for the transfer of funds.[81]

A case of advance fee fraud typically would play out in the following way. An offender makes unsolicited contact with an unsuspecting target via spam. He informs her that he is a Nigerian prince who has inherited a large sum of money from his late father, the king of Nigeria. He can make up an elaborate story about the instability of Nigerian politics which is threatening to dispossess him of his inheritance if he does not move it overseas. He asks the target to help him move this money to an international jurisdiction with the promise that he will share a portion of the inheritance with her.[82] Once the target has shown interest in the scam and has agreed to participate, she is instructed to make a series of miscellaneous payments[83] to the offender which will be used, supposedly, for cutting through the red tape associated with moving large funds. The amounts can increase as time goes by but, ultimately, the scam concludes with the promised share of the inheritance never materialising. To make matters worse, the target typically is left with no legal recourse because the transaction was illegal *ab initio*. The scam tends to cause severe financial and psychological harm.[84]

The advance fee fraud is referred to colloquially as the "419 Scam", having been named after provision 419 in the Nigerian Criminal Code which criminalises advance fee fraud. Nigeria is notorious for being a hub of this offence.[85] It is a common form of online fraud and it has mushroomed over the years, to include pyramid schemes, get-rich-quick

81 Cross, Smith & Richards (2014) at 1.
82 Neuhaus (2020) at 8.
83 SABRIC (no date) at 1.
84 Smith, Holmes & Kaufman (1996) at 3-5; Whitty (2018) at 98
85 Whitty (2018) at 97.

schemes, fraudulent business opportunities, fake educational qualifications, financial advice scams and lottery scams.[86]

Advance fee fraud is also one of the most discussed forms of online fraud, whether in the mainstream media, social media, popular culture or academic writings. One of the more famous scams was the *Banco Noroeste* scam, in which a Brazilian banker bought a fake airport for US$242 million from Nigerian fraudsters.[87] This story is discussed widely as an example of one of the biggest cyberfraud cases ever. However, while its sensational facts make for compelling reading, it is by no means a cybercrime.

Those who claim that advance fee fraud and its various manifestations are cybercrimes rely on the assertion that the internet is providing a huge marketplace for potential targets.[88] The increase in commercial and financial transactions conducted online has led to people being less prudent when it comes to sharing information online and responding to emails. Also, the convenience of internet transactions has robbed targets of the ability to observe social cues that might speak to the trustworthiness of the people with whom they interact. Further, the immediacy that comes with internet transactions has given offenders more avenues for committing fraud. Paradoxically, it appears that the lack of traditional authentication tools has spawned a lax attitude to security, creating more trust in the online system instead of healthy suspicion.[89]

Advance fee fraud occurs predominantly via email and the offender tends to find his victim by chance, as he would send millions of spam emails and only a handful of people respond positively. This means that he has a reach that defies geographical limitations. Here computers and the internet are crucial. They facilitate prolonged communication at minimal cost to the offender, which means that he can engage in multiple simultaneous scams. Still, the computer is not indispensable to the success of this crime. Before the advent of the internet, this type of fraud was perpetrated just as effectively via the telephone or snail-mail[90] or, as was the case in the *Banco Noroeste* scam, via face-to-face meetings. In other

86 Clough (2015) at 214.
87 BBC News Africa (2004) at 1.
88 Clough (2015) at 211.
89 Finch (2007) at 38.
90 Rich (2017) at 211.

words, advance fee fraud is a computer-enabled offence and does not warrant classification as a cybercrime.

4.3.3.3 Click Bait

Click bait scams are very common on the internet. The profitability of this scam is derived from exploitation of the way in which advertising on the internet is structured. Many websites and digital platforms depend on advertiser fees to operate and to make a profit. A website would charge advertisers certain fees depending on the amount of internet traffic which that website receives. This is determined by the number of clicks that a website receives per hour, per day, per week and so forth.[91] The more users visit a website, the more it can charge advertisers, thereby increasing its revenue from advertising. Click baiting is about luring users into visiting a website.

Click bait scams should not be conflated with "malvertising". A malvertising attack is a form of internet advertising which hides malware within advertisements that are hosted on relatively safe websites. The aim of malvertisements is to entice a target to click on a bogus advertisement which would download malware surreptitiously onto the computer system of the target.[92] This type of attack uses a similar concept to click bait, but it should not be considered as a form of fraud because the intention of the offender is not to defraud the target but to infect her system with malware so that he can gain some other benefit, for example, access to confidential information such as passwords and financial details.

Click baiting relies heavily on the manipulation of the target. It can come in the form of overstating or misrepresenting a news headline to bait people into clicking on a story. It does this by using hyperboles and superlatives that arouse the target's curiosity about an item. Invariably, the content of that item does not warrant such exaggeration.[93] Click bait schemes are common on social networking and social media platforms where one encounters headlines such as: "This girl gave a homeless man her lunch. You won't believe what happened next!" It is very likely that what happened next was that the homeless man

91 Clough (2015) at 216.
92 Techopedia (2018) at 1.
93 Gardner (2015) at 1.

thanked her and ate the sandwich, but the objective was to pique the target's curiosity and have her click on the story, much to her disappointment.

Unfortunately, as common as these tricks are, they are nothing new and are not exclusive to the internet. A classic example of sensational banners is the 1983 *New York Post* headline that declared: "Headless body found in topless bar", which is acclaimed for being as witty as it is horrific.[94]

Classifying click baiting as a form of cyberfraud is quite a stretch of the imagination. In fact, it hardly can be classified even as regular fraud. If we recall the elements of fraud, we note that there is indeed an intentional misrepresentation on the part of the perpetrator, but it is not clear where the actual or potential prejudice lies. At worst, a "victim" suffers disappointment that her expectation of being shocked by what happened between the homeless man and the girl is dashed. Sensationalism is hardly a crime. In any case, even if this were to be branded successfully as a case of offline fraud, the computer and the internet are simply enablers of the offence. All that has happened is that the offence has moved from the pages of sensationalist newspapers and magazines to an internet website.

4.3.3.4 Fraudulent Investments

The ease with which one can generate an impressive website that solicits investments and promises high returns has made fraudulent investment schemes very popular. This offence involves the rapid dissemination over the internet of fraudulent and misleading information regarding investment opportunities. It usually is done with the intention of influencing the share prices of companies. These schemes are called "pump and dump" or "trash and cash" schemes. Their tactics include releasing false news reports about certain shares and talking them up in online platforms.[95]

In the cryptocurrency market, drivers of pump and dump schemes tend to organise online on encrypted messaging platforms such as Telegram. They form what is called "pump groups" which are groups or channels on Telegram where investors would be invited to join via social media platforms. When preparing for a planned pump, the group administrator

94 New York Post (2015) at 1.
95 Li, Shin & Wang (2021) at 1..

would announce the time, date and exchange usually atleast a day in advance. The identity of the target token does not get announced until the scheduled time but members would get multiple reminder messages before the target token is announced. These kinds of operations do not last longer than a few minutes leaving non-members little to no time to participate.[96]

The rise of cryptocurrency and social media has created an additional dynamic to the scheme because they are admittedly faster than conventional manipulation of the stock market.[97] However, regardless of how fast or efficient the commission of the crime is, it does not change the essence of the crime. At its core, it is still computer enabled.

Arguments can be made for raising a philosophical debate of whether smartphones and by extension social media and platforms such as Telegram form part of the definition of a computer for purposes of the differentiating between computer enabled and computer dependent crimes. Such debate, unfortunately, is beyond the scope of this study.

Understanding the great impact in financial loss this type of scheme has on outside investors in a matter of minutes,[98] the fraud remains the same; artificially drive up the price of stocks, make money and then dump.

The internet may have provided a bigger and better platform to trick targets, but the scam was not dependent on the presence of a computer to be successful. It is a computer enabled crime if the advertisements that helped inflate the value of the shares were run predominantly over the internet. Should that be the case, the computer or internet merely offered the offenders a wider platform to reach more victims. It might be tempting to label the fraud a cybercrime because of the enormous financial reward that the offenders gained. However, this type of crime can be (and evidently has been) committed without resorting to cyberspace. Undoubtedly, it is a very sophisticated scheme which has the potential of taking full advantage of technological advancements, but currently it remains computer enabled. One can see a future in which fraudsters use botnets or artificial intelligence to perpetrate this type of offence, making it computer dependent. In that case,

96 Li, Shin & Wang (2021) at 1.
97 Li, Shin & Wang (2021) at 1.
98 Li, Shin & Wang (2021) at 18.

it may be a cybercrime, but it likely would be a case of cyberforgery and uttering, where the offender creates false data or computer programmes. In any case, fraudulent investment schemes can be dealt with adequately under the common law at this juncture.

4.3.3.5 Identity Theft

The terms "identity theft", "identity fraud" and ''identity crime" usually are used interchangeably because there is no generally accepted definition of the crime. The Australasian Centre for Policing Research has produced the following classification:

1. *Identity crime* is a generic term used to refer to offences where the defendant uses a false identity to perpetrate the crime. This may include such offences as money laundering, drug trafficking, tax evasion, illegal immigration or terrorism. It may also include lesser offences such as minors using false identification to buy alcohol.
2. *Identity fraud* is a more specific form of identity crime where a false identity is used to gain money, goods, benefits or services.
3. *Identity theft* is the assumption of pre-existing identity.[99]

Identity crime is by no means a new form of criminality but the advent of the internet has expanded its scope and provided new opportunities for offenders to acquire the targeted identity information.[100] The portability and transferability of digital data increase the desirability of the target while reducing the potential for detection.

Before the convenience of the internet, identity fraudsters used to rely upon "dumpster diving". This is the practice of rummaging through physical trash cans to find identification information from discarded documents, such as financial statements, confidential business letters and memoranda. Today, dumpster diving is not limited to physical trash but includes poorly sanitised and discarded hard drives which are flush with files containing sensitive information.[101]

The fears around identity fraud are exacerbated by the continuous stream of reports of massive data leaks which appear in the media every other day. In these data breaches —

99 Australasian Centre for Policing Research (2006) at 9-10.
100 Clough (2015) at 219.
101 Bonsla, Kunwar & Gupta (2019) at 20.

such as the one at Equifax, the American credit reporting agency, in late 2017 — there is always a concern about the use to which the sensitive information can be put by hackers.[102] However, once one wades through the sensationalism and the media frenzies, one realises that the fraud being perpetrated is the same as ordinary fraud. The use of sensitive personal information to commit credit card fraud, for example, has not changed since the traditional dumpster divers of yesteryear. Granted, the latter-day fraudsters possess better skill sets but they are conventional fraudsters just the same. They use the information they obtain in the same way as before. When one considers identity theft, one must differentiate between the hacking offences that may occur when the offender seeks to gain the confidential information and the fraudster who uses that information to defraud the target. The fraudster can be dealt with adequately under the common law.

4.4 Summation

The crime of fraud has evolved over the decades, but it has done so only in respect of the manner in which the fraudster perpetrates the crime. The essential elements of fraud have not changed in any significant way. There is a need to be vigilant when determining which offences are categorised as cybercrimes by observing minimum characteristics of the offence, such as whether it is computer enabled or computer dependent. In many cases an offence can be dealt with adequately in terms of the existing common law of fraud. If that is possible, the creation of a new crime of cyberfraud is unnecessary and will increase the burden on law enforcement agencies and the rest of the criminal justice system. It also will divert resources from detecting, combating and defeating true cybercrimes.

The crimes discussed above may have devastating effects on their victims, but they should not be re-classified arbitrarily as cybercrimes. It is important to allow the Cybercrimes Act to be effective by not saddling it with an overly broad mandate. Section 8 of the Cybercrimes Act ought not to be enacted until such time as it differentiates the crime of cyberfraud clearly from common-law fraud.

It is accepted that laws influence heavily the perception of society about what acts are right or wrong, socially acceptable or morally reprehensible. This is why crimes are set out clearly in legislation. But in order for any law to be effective in combating crime, its

102 Zou, Schaub (2018) at 2.

parameters must be defined clearly. In this regard, it is necessary to have minimum requirements or characteristics which identify what should qualify as a cybercrime and what should not.

Firstly, how can one combat something which one does not know how to define? It has been established that cybercrime grows at an exponential rate, and perhaps this has made legislators anxious to criminalise everything dubbed "cyber" without a proper evaluation of its cybercriminological veracity. The examples discussed above are evidence of that legislative anxiety.

Secondly, the complexity of cybercrime requires a phenomenal amount of resources to combat it. Many law enforcement agencies, such as the FBI and Interpol, have dedicated investigative units that deal specifically with cyber-related crimes. The Cybercrimes Act provides for the establishment of the Designated Point of Contact which will be housed within the existing structures of the South African Police Service (SAPS) as discussed in Chapter Six below.[103] Specialised units such as these need to have a clear mandate about the kinds of crimes which fall within their remit. For example, if a team within SAPS were to be made responsible solely for the cybercrimes contained in the Cybercrimes Act, the novelty of cybercrime almost guarantees an understaffed and/or under-skilled team with very limited resources.

Say a victim is hit over the head with a computer and she dies. Will that be called cybermurder? Of course not. The definition of murder in the common law is the unlawful and intentional killing of a person.[104] The manner in which the person is killed is inconsequential in the determination of whether a murder was committed. The victim could have been killed as easily with a brick, a hammer or a knife. The common-law crime of murder can address this case adequately. It obviously would not be the responsibility of any cybercrimes unit.

Take a second example. A target is sent an email telling her that she has won a prize of R50 000 and she would have to deposit R5 000 into the bank account of the sender as transactional fees. The victim complies but the R50 000 does not materialise. Is this a

103 Section 52 of the Cybercrimes Act.
104 Burchell (2016) at 77.

cybercrime and should a special cybercrimes unit be investigating it? Undoubtedly, this is a case of fraud but it does not qualify as a cybercrime. The crime may have been enabled by a computer but it is definitely not computer dependent.

The distinction between computer enabled and computer dependent crimes is important in these cases because it helps with the distribution of resources. Many computer enabled crimes, such as advance fee frauds, are just high-tech manifestations of offline crimes, which means that the work of the fraudster is made easier and more efficient by a computer. She can reach more people and more places in less time than if she had to defraud one person at a time. However, the inclusion of the email as a medium is not enough to elevate this crime to the status of a cybercrime and, therefore, these cases may be referred to an ordinary crimes unit which deals with conventional offline cases. The problem described above applies not only to the police services but also to the prosecuting authorities, as well as to cybercrime and cybersecurity researchers. The difficulty is that cybercrime is becoming so mythologised that cases which may be dispensed with easily under the common law are being “complexified” and end up not being resolved at all.

CHAPTER FIVE

PROCEDURAL REGIME

5.1 Introduction

In order to relate the substantive matters pertaining to the motivated offender and the suitable target to the legal responses of the capable guardian in Chapter Six below, it is necessary in this chapter to deal with the procedural aspects of combating cybercrime. The procedural regime also provides the background needed for understanding some of the duties with which the proposed cyber-capable guardian would be tasked.

Before a motivated offender can be brought to justice, a state must determine whether it has the jurisdiction to prosecute the offence in question. Once a state has determined that it has jurisdiction to prosecute, it can begin with investigations. The nature of cybercrime, however, almost guarantees that investigators will have to deal with cross-border offences which require to be combatted with strong international co-operation and mutual assistance mechanisms. This chapter seeks to determine the international perspective on jurisdiction, international co-operation and mutual assistance, as provided for in the Budapest Convention, and then to compare that perspective to the procedural measures contained in the Cybercrimes Act.

5.2 Jurisdiction

Jurisdiction is one of the key elements in the fight against cybercrime, given that the chances of a cybercrime being transnational are much higher than for most other crimes. It presents numerous jurisdictional conflicts, both positive, as where several states claim jurisdiction at the same time, and negative, where no state claims jurisdiction.

There are several discrete concepts that are encompassed in jurisdiction. These are jurisdiction to prescribe (authority of a state to make law), to adjudicate (authority of a state to apply the law) and to enforce (authority of the state to compel compliance with the law).[1] As a sovereign power, a state has the jurisdiction to prescribe the authority that it has to make laws which will apply to the activities of its citizens by way of legislation and the scope

1 Dodge (2020) at 5.

of the executive orders, administrative rules or judicial determinations. Jurisdiction to adjudicate refers to the state's authority to preside over persons or entities through the judicial or the administrative arms of the government in order to determine whether there have been any violations of the prescribed laws. Jurisdiction to enforce is the state's authority to induce or compel persons and entities to comply with the prescribed laws and, in the absence of such compliance, it is the state's authority to impose an appropriate punishment.[2]

Central to international jurisdiction is the principle of territoriality.[3] This principle derives from the basic concept that every sovereign state has the lawful authority to exert control over everything within its territory, generally to the exclusion of other states.[4] Factors such as the place where the act was committed, the country where the motivated offender is resident, the location where the effect of the crime was felt, the country where the suitable target resides, or all of these together are most helpful.[5]

One of the early cases which illustrates jurisdictional challenges well is the saga of the Love Bug virus. In 2000, the Love Bug virus was released onto the internet and it was estimated to have infected more than forty-five million users in over twenty countries within two hours and to have caused between two and ten billion dollars in damage. The origins of the virus were traced to the Philippines, where one Onel de Guzman was identified by the FBI and the Philippines Bureau of Investigation as the creator of the virus. A challenge facing the investigating authorities was that, at the time, the dissemination of the virus was not a crime in the Philippines. This made it difficult for the FBI to obtain arrest warrants which would enable its agents to search Guzman's apartment for evidence pertaining to the creation and dissemination of the virus. Furthermore, once they had obtained the search warrant and had arrested Guzman, they were faced with the challenge of how they could prosecute Guzman in the Philippines when the creation and dissemination of a computer virus was not a crime there. The only avenue the authorities had was to charge Guzman with fraud and credit card theft on the premise that the virus was meant to harvest user passwords for obtaining internet services and other items of

2 Brenner & Koops (2004) at 5-6.
3 Ryngaert (2016) at 52.
4 Ryngaert (2016) at 51.
5 Brenner & Koops (2004) at 3.

value. Unfortunately, these charges turned out to be legally insufficient and his prosecution in the Philippines failed. Furthermore, because he could not be prosecuted in the Philippines, it was determined also that he could not be extradited for prosecution to the United States or any other country where the effects of the Love Bug virus were felt.[6]

The modern conception of jurisdiction is that a state has jurisdiction over any conduct which takes place wholly or substantially within its territory. Where the conduct does not occur within its territory, a state still can assume jurisdiction if the effects of the conduct are intended to have a substantial effect on its territory.[7] Additionally, a state always has jurisdiction over its nationals regardless of whether they are inside or outside its territory. It also has jurisdiction over two kinds of foreign persons or entities: the first are those inside its territory and the second are those that are outside its territory but engage in activities which threaten its security or a limited class of its interests.[8] However, the expanded notion of jurisdiction does not mean that a state may exercise jurisdiction over a person in another state if it is unreasonable to do so.[9]

Reasonableness is an important consideration because, while a state may have legitimate interests which it is trying to protect by regulating certain activities, it must do so with due regard for another state's sovereignty. If, for instance, two states have criminalised an offence and state A has agreed to prosecute a motivated offender at the behest of state B, it may be unreasonable for state B to prescribe to state A how it should conduct the prosecution or what sentence its courts should hand down — subject, of course, to diplomatic agreements or human rights considerations, such as whether the death penalty is an appropriate sentence.

There are various factors that may be employed to test whether the exercise of jurisdiction to prescribe is unreasonable or not. The first is to ascertain the extent of the link between the prohibited activity and the direct, substantial or foreseeable effect on the state's territory. The second is to consider the factors such as the nationality or residence of a motivated offender to determine the connections that may exist between her and the regulating state. The third is to determine the character of the activity regulated by asking

6 Brenner & Koops (2004) at 7.
7 Brenner & Koops (2004) at 8. See also August (2002) at 534.
8 Dodge (2020) at 7.
9 Brenner & Koops (2004) at 8; Dodge (2020) at 4.

whether it is desirable for it to be regulated, how other states have dealt with the activity, whether there exist interests which may be protected or hurt by legislation, and how important the regulation is in the international political, legal or economic ecosystem. And finally, reasonableness may be adjudged by determining whether the regulations meet international norms and standards.[10]

The issue of reasonableness is an important one because, as will be seen shortly, the Cybercrimes Act tends to stretch the traditional concept of jurisdiction in some instances. It does so by not even requiring that the effects of an offence be felt within South Africa for it to exercise jurisdiction over that offence.

Another key determinant of jurisdiction is the principle of dual or double criminality. This principle requires that the unlawful conduct over which a state wants to claim jurisdiction be a crime in both or all of the states involved, particularly if extradition is to be permitted.[11] For instance, what would happen if an adult content website in Country A were to expand its reach into Country B where adult websites are unlawful? Could the owner of the website in Country A be arrested and indicted in Country B for spreading pornographic material even though she has not done direct business there? Furthermore, what happens if the age of consent in Country A is 16 years and some of the adult material on the website contains sexual content of a 17-year-old? If the age of consent in most other countries is 18 or 21 years, does this mean that the website owner is liable for prosecution in all those countries for spreading child pornography?

The principle of dual criminality is important because, in this example, a citizen of Country A could be prosecuted by the authorities of Country B for perfectly legal conduct that would have occurred wholly within the territory of Country A but, because it is on the internet, it may have violated the laws of Country B. If this eventuality were to be allowed, it would undermine the sovereignty of Country A to exercise authority over its own citizens and others within its borders.[12] However, the principle of dual criminality, as well as the proposition that a nation has sovereign authority over people within its borders, is not

10 Brenner & Koops (2004) at 9.
11 Brenner & Koops (2004) at 7; Zając (2021) at 2.
12 Brenner & Koops (2004) at 7.

absolute. Over the past number of years, it has been expanded to cater for the common phenomenon of persons offending in a territory in which they are not physically present.[13]

5.2.1 The Budapest Convention and Jurisdiction

Article 22 of the Budapest Convention deals with jurisdiction. It provides that:

> (1) Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
> (a) in its territory; or
> (b) on board a ship flying the flag of that Party; or
> (c) on board an aircraft registered under the laws of that Party; or
> (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
> (2) Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1(b) through 1(d) of this article or any part thereof.
> (3) Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
> (4) This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
> (5) When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Article 22(1)(a) is based on the principle of territoriality. Each Party is required to punish the commission of a crime that is committed in its own territory. Subparagraphs Article 22(1)(b) & (c) are based on a variant of the principle of territoriality, which requires jurisdiction to be asserted over ships flying the flag of that Party or an aircraft registered under the laws of that Party. This obligation already is implemented as a general matter in the laws of many states, as ships and aircraft generally are considered to be extensions of the territory of a state.[14]

Article 22(1)(d) is based on the principle of nationality. This principle provides that nationals of a state are obligated to comply with that state's domestic laws, even when they are outside its territory. In other words, if a national of Party A commits an offence in the

13 Brenner & Koops (2004) at 8.
14 Budapest Convention, Explanatory Report at 40.

territory of Party B, Party A can prosecute if the conduct is also an offence under the laws of Party B where the offence was committed. This principle is applied most commonly by states that adhere to the civil law tradition.[15]

Article 22(2) permits Parties to enter a reservation to the jurisdictional grounds that are laid down in Article 22(1)(b)-(d). However, Parties may not enter a reservation with respect to the establishment of territorial jurisdiction under Article 22(1)(a) or if the obligation falls under the principle of *aut dedere aut judicare* (extradite or prosecute) under Article 22(3). Article 22(3) is an important provision because it ensures that Parties which refuse to extradite a national have the legal ability to investigate and prosecute the person domestically, in place of the Party which requested extradition.[16]

Because of the nature of cybercrimes, it is often possible for multiple states to assert jurisdiction over a single offence, as in the case of a DDoS attack. In order to avoid duplication of efforts or even competition amongst law enforcement agencies, states are encouraged to consult one another in order to ensure that the investigations are efficient and that proceedings are fair, as well as to determine where prosecution will take place. It is permitted also, under Article 22(5), for Parties either to choose a single location for prosecution or to agree upon the separation of cases, where Party A prosecutes some and Party B prosecutes others. The obligation to consult is not absolute but is to be operationalised where it is appropriate to do so.[17]

5.2.2 The Cybercrimes Act and Jurisdiction

Chapter 4 of the Cybercrimes Act provides for jurisdiction over offences committed in terms of the Act. Chapter 4 consists of a single section, section 24. To begin with, section 24(1) reads:

> A court in the Republic trying an offence has jurisdiction where—
> (a) an offence in terms of Part I or II of Chapter 2 was committed—
> (i) in the territory of the Republic; or
> (ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time the offence was committed;

15 Budapest Convention, Explanatory Report at 41.
16 Budapest Convention, Explanatory Report at 41.
17 Budapest Convention, Explanatory Report at 41.

(b) an offence in terms of Part I or II of Chapter 2 was committed, in the Republic, or outside the Republic, against a person who is citizen of the Republic or ordinarily resident in the Republic;
(c) an offence in terms of Part I of Chapter 2 was committed, in the Republic, or outside the Republic, against a person who is—
    (i) a company, incorporated or registered as such under any law, in the Republic; or
    (ii) anybody of persons, corporate or unincorporated, in the Republic;
(d) an offence in terms of Part I of Chapter 2 was committed, in the Republic, or outside the Republic, against—
    (i) a restricted computer system contemplated in section 11(1)(b); or
    (ii) a government facility of the Republic abroad, including an embassy or other diplomatic or consular premises, or any other property of the Republic; or
(e) any act in preparation of an offence in terms of Part I or II of Chapter 2 or any action necessary to commit the offence took place—
    (i) in the territory of the Republic; or
    (ii) on board a vessel, a ship, an off-shore installation, or a fixed platform, or an aircraft registered or required to be registered in the Republic at the time the offence was committed.

The Cybercrimes Act provides for territorial jurisdiction in similar terms to the Budapest Convention. Section 24(1) provides for the overall scope of jurisdiction that will be exercised over offences committed in Part I and II of Chapter 2 of the Cybercrimes Act.

Section 24(1)(a) stipulates that South African courts have jurisdiction over any offence that is committed within the borders of South Africa. Furthermore, where the Budapest Convention provides for the exercise of jurisdiction over any offence committed aboard a ship flying the territory's flag or an aircraft registered to that territory, the Cybercrimes Act expands the list to include a vessel, an offshore installation and a fixed platform belonging to South Africa. This provision is related closely to section 24(1)(e) as it is formulated in similar terms except it provides for the any act in preparation of committing an offence in Part I or II of Chapter 2.

Section 24(1)(b) provides for offences committed either inside or outside the territory of South Africa but committed against a suitable target who is either a citizen of South Africa or ~~is~~ ordinarily is resident in South Africa. Section 24(1)(c) is similar to section 24(1)(b), except that it applies only to offences provided for in Part I of Chapter 2. It goes further than what the Budapest Convention contemplates by extending the protection to include juristic persons registered under any law in South Africa.

Section 24(1)(d) also applies only to offences contained in Part I of Chapter 2. It provides for the exercise of jurisdiction over offences which threaten the country's critical

information infrastructure as contemplated in section 11(1)(b) of the Cybercrimes Act. This includes government facilities which are outside the borders of South Africa, such as embassies, consulates and the like.

Section 24(2) and section 24(3) of the Cybercrimes Act provide that:

(2) If the act alleged to constitute an offence in terms of Part I or II of Chapter 2 was committed outside the Republic, a court of the Republic, regardless of whether or not the act constitutes an offence at the place of its commission, has jurisdiction in respect of that offence if the person to be charged—
  (a) is a citizen of the Republic or ordinarily resident in the Republic;
  (b) was arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic at the time the offence was committed;
  (c) is a company, incorporated or registered as such under any law, in the Republic; or
  (d) Anybody of persons, corporate or unincorporated, in the Republic.

(3) Any act alleged to constitute an offence in terms of Part I or II of Chapter 2 and which is committed outside the Republic by a person, other than a person contemplated in subsection (2), is, regardless of whether or not the act constitutes an offence or not at the place of its commission, deemed also to have been committed in the Republic if that—
  (a) person is found to be in South Africa; and
  (b) person is for one or other reason not extradited to, or by South Africa, or if there is no application to extradite that person.

Sections 24(2) & (3) may be read together as they both speak to the principle of dual criminality albeit not directly. Section 24(2) provides that if an offence in terms of Part I or II of Chapter 2 is committed outside the country by a South African citizen, someone ordinarily resident in South Africa, or a foreigner caught in South Africa, then South African courts can exercise jurisdiction over it. This exercise of jurisdiction is possible even if the act does not constitute an offence in the place where it is committed.

Section 24(3) goes even further than section 24(2) to say that if any person who is not covered by section 24(2) has committed an offence under Part I or II of Chapter 2 outside of South Africa, she can be tried by South African courts regardless of whether or not the place where the act was committed considers said act to be an offence under its laws. The person is deemed to have committed the offence in South Africa if that person is not extradited or where there is no extradition application. It is important to note that both conditions must be met, that is, apprehension in South Africa and the absence of extradition processes. Thus, for example, if a motivated offender commits an offence in Namibia which is yet to enact cybercrime legislation, she can be charged under the Cybercrimes Act if she is

a South African citizen or resident. Furthermore, the wording of Section 24(3) suggests that if a Namibian citizen or resident commits an offence contemplated in Part I or II of Chapter 2 of the Cybercrimes against a Namibian suitable target in the Namibian territory, she may be charged and prosecuted in South Africa if she is apprehended in South Africa and not extradited.

Section 24(2) and section 24(3) are expressions of a country's inherent jurisdiction to prescribe. There are no provisions in the Budapest Convention which are similar to these. The South African provisions do not mention the application of the principle of dual criminality. And they are so far-reaching that the offence need not even be committed in South Africa nor have its effect felt here. The mention of extradition, however, is an indication that there must be some level of international co-operation. It is here where one must consider whether this exercise of power is reasonable. On the one hand, it ensures that no cybercrime goes unpunished. On the other hand, it is debatable whether the courts would be successful in prosecuting an offence which has no connection to the country except that the motivated offender is apprehended here. It would be a difficult and most likely expensive task to gather evidence outside the country, for example. One would seriously have to consider whether the benefits truly outweigh the costs.

Section 24(2) and section 24(3) must be read together with section 24(5),[18] which provides that the decision to prosecute under these circumstances must be made with the express permission of the National Directory of Public Prosecutions. This is an indication that such decisions should not be taken lightly, so as to avoid diplomatic challenges. One can imagine a situation where the offence is high profile in nature and multiple states want to assume jurisdiction. The decision to assume jurisdiction must be authorised by the highest South African prosecutorial agency.

Section 24(4) of the Cybercrimes Act provides that:

> Where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or

18 The section reads:
(a) A prosecution in terms of subsections (2) and (3)—
  (i) may only be instituted against a person with the written permission of the National Director of Public Prosecutions; and
  (ii) must commence before a court designated by the National Director of Public Prosecutions.
(b) A copy of the written permission and designation must be served on the accused and the original thereof must be handed in at the court in which the proceedings are to commence.

> as an accessory after the offence, the offence is deemed to have been committed not only at the place where the act was committed, but also at every place where the person acted.

Section 24(4) provides for jurisdiction over inchoate offences in similar terms to section 17. It specifies that the offence is deemed to have been committed not only at the location where the act actually was committed but also at every other location where the accused acted. The phrasing is helpful because it ensures that every stage of the planning and execution of the offence is covered.

An interesting question is whether the "criminal" location would be limited to the physical place where the motivated offender acts. For example, if a motivated offender is located physically in Namibia but uses a server located in South Africa to attack a suitable target located in Lesotho, does South Africa have jurisdiction? Furthermore, if the use of the South African [spacing] server fails but the motivated offender succeeds by using one in Serbia, will South Africa still be entitled to assume jurisdiction? One may assume that the answer to both questions would be yes, considering how widely the power to assume jurisdiction has been formulated in this section.

Finally, section 24(6) of the Cybercrimes Act informs us that:

> The National Commissioner and the National Head of the Directorate, respectively, in consultation with the National Director of Public Prosecutions must issue directives, with which all police officials must comply in the execution of their functions in terms of this Act regarding the investigation of offences that was [sic] committed outside the Republic.

This section seeks to regulate the investigation by South African police officials of cybercrimes committed in foreign countries. It provides that the National Commissioner of the SAPS and the National Head of the Directorate for Priority Crime Investigation must consult with the National Director of Public Prosecutions to issue directives for all police officials who investigate offences which are committed outside the South Africa. These directives will govern the police's abilities to co-operate with police officials of other jurisdictions.

5.3 International Co-operation

International co-operation in the Budapest Convention is viewed through two lenses: the first is extradition[19] and the second is mutual assistance.[20] By contrast, the Cybercrimes Act views international co-operation against cybercrime primarily through the lens of mutual assistance.

The general principles of international co-operation in the Budapest Convention require Parties to co-operate with one another to the widest extent possible and in keeping with relevant international instruments, uniform or reciprocal legislation and domestic laws for purposes of investigations or criminal proceedings relating to cybercrime.[21] Further, where a requested Party makes dual criminality a condition for mutual assistance, the condition is deemed to be fulfilled if the conduct underlying the offence for which the assistance is sought is a criminal offence under its laws, even if the offence is not placed in the same category or is not described in the same terminology as the offence in question.[22] This provision was included to ensure that Parties do not adopt too rigid a test, especially considering the many differences in legal systems, variations in terminology and categorisation of criminal conduct.[23] As is evident from the discussion in §5.2.2 above, dual criminality is not an issue as far as the Cybercrimes Act is concerned, and hence not an obstacle to international co-operation.

5.3.1 Extradition

Article 24 of the Budapest Convention allows for extradition for the criminal offences, provided that the offences are punishable under the laws of both Parties by a prison sentence of at least one year or a more. Where there are different minimum sentences prescribed in the respective jurisdictions, the Parties are at liberty to enter into agreements on the basis of uniform or reciprocal legislation or under an extradition treaty, including the European Convention on Extradition. The minimum penalty provided for under such a treaty then is applicable to the cybercrime in question.[24]

19 Article 24 of the Budapest Convention.
20 Article 25 of the Budapest Convention.
21 Article 23 of the Budapest Convention.
22 Article 25(5) of the Budapest Convention.
23 Budapest Convention, Explanatory Report at 45.
24 Article 24(1)-(2) of the Budapest Convention.

The Budapest Convention provides that where a Party requires an extradition treaty before agreeing to extradite and where no such treaty exists, the Party may consider the Convention itself as the legal basis of extradition for any criminal offences as provided for in Article 24(1). Parties which do not make extradition conditional on the existence of a treaty are required to recognise the offences contained in the Convention as extraditable offences between themselves. Extradition and grounds for refusal of a request for extradition are governed by the laws of the requested Party or by applicable extradition treaties.[25]

Where a request for extradition is refused solely on the basis of nationality or where the requested state considers that it has jurisdiction over the offence, it must submit the case, at the instance of the requesting state, for domestic prosecution. Also, it must report the outcome of the prosecution to the requesting Party.[26]

The Cybercrimes Act does not have a provision dedicated to the question of extradition, except to confirm jurisdiction in terms of section 24(3) of the Act. The drafters of the Act may have thought that it was not necessary to deal extensively with the question of extradition, because South Africa does have a dedicated Extradition Act,[27] which contains detailed provisions regarding extradition and which makes reference to the International Co-operation in Criminal Matters Act[28] (ICCMA).

5.3.2 Mutual Assistance

Article 25 of the Budapest Convention provides for the general principles of mutual assistance. It requires, *inter alia*, that states adopt the legislative and other measures needed to comply with Articles 27 to 35.[29] As with international co-operation, Parties are

25 Article 24(3)-(5) of the Budapest Convention.
26 Article 24(6) of the Budapest Convention.
27 Act 67 of 1962.
28 Act 75 of 1996.
29 Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements;
Article 28 –Confidentiality and limitation on use;
Article 29 – Expedited preservation of stored computer data;
Article 30 – Expedited disclosure of preserved traffic data;
Article 31 – Mutual assistance regarding accessing of stored computer data;
Article 32 – Trans-border access to stored computer data with consent or where publicly available;
Article 33 – Mutual assistance in the real-time collection of traffic data; and
Article 34 – Mutual assistance regarding the interception of content data.

enjoined to provide one another with mutual assistance to the widest extent possible for cybercriminal investigations and prosecutions.[30] Mutual assistance is to be extensive and impediments have to be limited strictly. Furthermore, the obligation to provide mutual assistance applies both to criminal offences relating to computer systems and data and to the collection of evidence, in electronic form, of a criminal offence.[31]

Mutual assistance in the Cybercrimes Act is dealt with in Chapter 5, specifically in sections 46 to 51. Section 46 states that the provisions of sections 48 to 51 apply in addition to Chapter 2 of the ICCMA. [32] It provides further that these provisions also relate to the preservation of any evidence regarding the commission or suspected commission of offences provided for in the Act. Sections 48 to 51 apply pending a request in terms of the ICCMA.

5.3.2.1 Spontaneous Assistance

Section 47 of the Cybercrimes Act empowers the National Commissioner of the SAPS or the National Head of the Directorate for Priority Crime Investigation spontaneously to furnish any information obtained during an investigation to a law enforcement agency of a foreign state, if he or she is of the opinion that the disclosure may assist said foreign state to commence or carry out the investigation of an offence or lead to further co-operation between the states. They may do so subject to conditions of confidentiality and other limitations of use as they see fit.[33] These conditions apply equally to the SAPS receiving similar information from a foreign state.[34]

This approach is in keeping with Article 26 of the Budapest Convention which provides that a Party may forward to a fellow Party any information it has obtained during an investigation, even in the absence of a request for mutual assistance. This spontaneous assistance has to be in keeping with what is permissible in the domestic laws of the providing Party.[35] The providing Party may request that the receiving Party treat the

30 Article 25(1) of the Budapest Convention.
31 Budapest Convention, Explanatory Report at 44.
32 For a comprehensive discussion of the International Co-operation in Criminal Matters Act, see Mujuzi (2015) at 351.
33 Section 47(1) of the Cybercrimes Act.
34 Section 47(2) of the Cybercrimes Act.
35 Article 26(1) of the Budapest Convention.

information as confidential or adhere to any other specific conditions. If the receiving Party cannot accept the conditions, it must inform the providing Party, and if it accepts the conditions, it is bound by them.[36]

5.3.2.2 Requesting Mutual Assistance

Article 25 of the Budapest Convention provides that a request for mutual assistance is to be governed by the conditions provided for in the relevant domestic laws of the Parties, as well as the applicable mutual legal assistance treaties (MLATs) entered into by the Parties.[37] This provision is necessary to protect the rights of the subjects of the mutual assistance. For example, in a case where assistance for search and seizure is sought, a requesting Party must adhere to the fundamental requirements contained in the domestic laws of the requested Party.[38]

The Convention provides also that, in urgent cases, a request for mutual assistance may be submitted via various "non-traditional" means, such as fax and email, taking into account the appropriate levels of security and authentication required.[39] This provision caters for the volatility of computer data. Its objective is to ensure that the process of obtaining mutual assistance is accelerated so that critical information or evidence is not lost or deleted before a formal request is prepared, transmitted and answered. Parties therefore are empowered to make urgent requests for assistance through expedited means of communication rather than the traditional means which are much slower and arduous, because they involve sending written, sealed documents through diplomatic pouches or mail delivery systems. As technology advances, further expedited means may be developed and employed.[40] If required, a formal confirmation of the received request must follow.[41]

Section 51 of the Cybercrimes Act contains the procedure for requesting assistance from a foreign State. A magistrate may issue a direction requesting a foreign state to preserve data, seize data or disclose traffic data on an expedited basis, obtain real-time or

36 Article 26(2) of the Budapest Convention.
37 Article 25(4) of the Budapest Convention.
38 Budapest Convention, Explanatory Report at 45.
39 Article 25(3) of the Budapest Convention.
40 Budapest Convention, Explanatory Report at 44.
41 Article 25(3) of the Budapest Convention.

archived communication-related information or intercept direct communications in the jurisdiction of that foreign State.[42] The direction must specify that (a) there are reasonable grounds for believing that the offence contemplated in the Act has been committed in South Africa or it is necessary to determine whether it has been committed in South Africa; (b) an investigation in respect of said offence is underway; and (c) for purposes of the investigation and the interests of justice, it is necessary for the assistance specified in the direction be provided by the requested Party.[43] The direction must be sent to the National Director of Public Prosecutions (NDPP) for onward transmission to the appropriate authority or the Designated Point of Contact in the requested state.[44]

Section 48 of the Cybercrimes Act provides that a foreign state may request mutual assistance for the preservation and seizure of data or other article, the expedited disclosure of traffic data or other article, the obtaining of real-time or archived communication-related information, or interception of indirect communications from the Designated Point of Contact (DPoC) in South Africa.[45] The DPoC, in turn, must submit the request to the NDPP for consideration.[46] The NDPP must satisfy herself or himself that criminal proceedings have been instituted in the foreign state or there are reasonable grounds to believe that an offence has been committed in the foreign state which is similar or substantially similar to the offences provided for in the Cybercrimes Act.[47] Also, the NDPP must satisfy herself or himself that the foreign state intends to submit a form in terms of section 7 of the ICCMA[48] in order to obtain any data, information, communication or article from South Africa which it would use in its investigation or proceedings.[49] Thereafter, she or he must submit the request for assistance, together with her or his recommendations, to the Minister of Justice and Correctional Services for approval.[50] Once it has been approved, the NDPP must

42 Section 51(2) of the Cybercrimes Act.
43 Section 51(2) of the Cybercrimes Act.
44 Section 51(3) of the Cybercrimes Act.
45 Section 48(1) of the Cybercrimes Act.
46 Section 48(2) of the Cybercrimes Act.
47 Section 48(3)(i)-(iii) of the Cybercrimes Act.
48 Section 7 of ICCMA provides for foreign requests for assistance in obtaining evidence in criminal matters in similar terms to the Cybercrimes Bill, including that the Director-General must satisfy herself or himself that an offence has been committed in the requesting state.
49 Section 48(3)(iv) of the Cybercrimes Act.
50 Section 48(4)(a) of the Cybercrimes Act.

forward the request to the Designated Judge[51] for consideration.[52] Where the request relates to an expedited request for disclosure of data traffic, the NDPP must submit the request, together with her or his recommendation, directly to the Designated Judge. This is because neither subsections 3(a)(i)-(iv) nor (4) apply to this type of request.[53]

Given that the collection of data and the like may be intrusive upon the rights of the data subject, it is understandable why it may be necessary for a request for mutual assistance to undergo so many checks and balances. However, it is not immediately clear why a single request must go through the DPoC, the NDPP, the Minister of Justice and Correctional Services, and the Designated Judge for approval. With each stage of approval the likelihood increases that there will be significant time lags which, in the fight against cybercrime, defeats the purpose of speedy co-operation.

The borderless nature of cybercrime also means that one can anticipate that the DPoC will receive very many requests and, assuming that all the officials in the process apply their minds to the request at each stage, the process runs the risk of being grossly inefficient. It is not convincing that each official in this chain is necessary. It would be better if a request received by the DPoC is evaluated by a senior or designated police official who takes it to the Designated Judge for confirmation and approval. The Designated Judge will determine whether there are any serious issues with the request and address it accordingly.

5.3.2.3 Expedited Preservation of Stored Data

Article 29 of the Budapest Convention provides for the expedited preservation of stored computer data. Preservation is a limited provisional measure which is intended to take place much more rapidly than the execution of a traditional request for mutual assistance. This mechanism is essential for counteracting the volatility of computer data, as it ensures that

51 Section 1 of the Cybercrimes Act provides that the Designated Judge means a Designated Judge as provided for in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information (RICA) Act 70 of 2002. RICA defines a Designated Judge as "any judge of the High Court discharged from active service under section 3(2) of the Judges' Remuneration and Conditions of Employment Act 47 of 2001, or any retired judge, who is designated by the Minister to perform the functions of a designated judge for the purpose of this Act".

52 Section 48(4)(b) of the Cybercrimes Act.

53 Section 48(5) of the Cybercrimes Act.

the data is available pending mutual assistance requests which may take weeks or even months to conclude.[54]

Expedited preservation is beneficial not only because it is more rapid than ordinary requests for mutual assistance, but also because it is less intrusive in that the mutual assistance officials are not expected to take possession of the data from the custodian (usually an ISP or another third party). They may request that the custodian preserve data, that is, not delete it pending its being turned over to law enforcement for investigations. Since this mechanism does not involve the examination of data by or disclosure of data to investigators, it protects the privacy of the data subjects until compliance with the mutual assistance regimes have occurred. The aim is to have extremely rapid preservation of the data so that any irretrievable loss may be avoided.[55]

A preservation request, being an interim measure, will not be as detailed as the full mutual assistance request which will have to follow. The information contained in the preservation request will be in summary form and include the minimum required to process the request, but enough to identify the data and show how it is or will be relevant to an investigation, thereby justifying why preservation is necessary. Dual criminality is not a condition for a preservation order as it would be counterproductive in general, given that preservation is non-intrusive.[56]

A requested Party may refuse to execute a request for a preservation order if it is believed that the execution would have a negative impact on said Party's sovereignty or security, threaten the public order, or affect any other essential interest, for example, where the request is related to a political offence. No other bases for refusing a request for preservation are contemplated because of the centrality of preservation to the investigation and prosecution of cybercrimes.[57]

Parties are obligated to ensure that data preserved pursuant to Article 29 of the Budapest Convention is held for at least 60 days, pending the receipt of the formal request for mutual assistance regarding the disclosure of the data. This provision seeks to ensure

54 Budapest Convention, Explanatory Report at 50.
55 Budapest Convention, Explanatory Report at 51.
56 Budapest Convention, Explanatory Report at 51.
57 Budapest Convention, Explanatory Report at 51-2.

that the requesting Party is afforded enough time to submit a request for search, seizure or disclosure of data. Following the receipt of the request, the preservation of the data must continue, pending a decision on the execution of the request.[58]

Section 41 of the Cybercrimes Act provides that a specifically designated police official may issue an expedited preservation of data direction to any person, service provider or financial institution.[59] The official must believe, on reasonable grounds, that such person, service provider or financial institution is in possession of, is to receive or is in control of data which is relevant, because it was or may be used in the commission of an offence, or because it is data which has the purpose of committing or facilitating the commission of an offence or which may afford evidence of the commission of an offence.[60]

In terms of the Cybercrimes Act, the official must ensure that she gives due regard to the rights, responsibilities and legitimate interests of affected persons and that she acts in proportion to the severity of the offence in question.[61] The offences should be similar to those contemplated in Part I or II of Chapter 2 of the Act or should be offences which are substantially similar to offences which are recognised in South Africa but committed by means of or facilitated by the use of an article in a foreign state.[62] This also applies to archived communication-related information which a service provider no longer is required to store due to the lapse of time or any other data which must be stored for any other prescribed period of time.[63]

The direction for a preservation of data must be in the prescribed form and be served on the person, service provider or financial institution in the prescribed manner by a police official.[64] The direction must instruct the person, service provider or financial institution to (a) preserve the current status of the data, (b) not to deal in any manner with the data, or (c) deal in a certain manner with the data, from the time of service and for a

58 Article 29(7) of the Budapest Convention.
59 Section 41(1) of the Cybercrimes Act.
60 Section 41(1)(a)-(e) of the Cybercrimes Act.
61 Section 41(1) of the Cybercrimes Act.
62 Section 41(1)(iii) of the Cybercrimes Act.
63 Section 41(2) of the Cybercrimes Act.
64 Section 41(3) of the Cybercrimes Act.

period of 21 days.[65] This 21-day period may be extended for an additional period by way of a preservation of evidence order and the extension may not exceed 90 days.[66]

Should timeous or reasonable compliance with the preservation request not be possible, the affected person, service provider or financial institution may apply to a magistrate for an amendment or cancellation of the direction. The magistrate must consider the application, call for evidence if necessary, make a decision on the application, and inform the designated police officer of the decision.[67]

Finally, a person, an electronic communications service provider or financial institution which fails to comply with the request or makes false statements with regard to the request is guilty of an offence and may be punished with a fine or imprisonment not exceeding two years or both.[68]

5.3.2.4 Expedited Disclosure of Preserved Traffic Data

Article 30 of the Budapest Convention provides for the expedited disclosure of preserved traffic data.[69] This provision addresses the situation where Party A seeks to obtain traffic data which may have travelled through the computers of Party B during the commission of a crime so that it can trace the transmissions to the source and thus identify the perpetrator or locate critical evidence. This exercise can help determine whether data found in Party A's territory has been routed via a service provider from Party B or whether it originates from a service provider in Party A. In this case as well, time is of the essence because determining the details of traffic data will assist in requests for preservation of stored data and other forms of mutual assistance from another Party. If the transmission is determined to have originated from the requesting Party, it would be able to secure the preservation and disclosure of further traffic data through its domestic laws. As with the preservation of stored data, a requested Party may refuse a request for disclosure of preserved traffic data only if execution is likely to prejudice its sovereignty and other essential interests.[70]

65 Section 41(4) of the Cybercrimes Act.
66 Section 41(6) of the Cybercrimes Act.
67 Section 41(7)-(8) of the Cybercrimes Act.
68 Section 41(9) of the Cybercrimes Act.
69 Article 30 is the international equivalent of Article 17 of the Convention.
70 Budapest Convention, Explanatory Report at 52.

Section 44 of the Cybercrimes Act provides for a disclosure of data direction and search for, access to and seizure of articles subject to a preservation of evidence direction. It specifies that where an expedited preservation of data direction is in place and it is expedient to obtain the data without a search warrant, a magistrate (subject to various provisions)[71] may issue a disclosure of data direction if there are reasonable grounds for believing that a person, service provider or financial institution may receive, is in possession of, or is in control of data which is relevant to offences provided for in the Act.[72] Section 44(2) sets out the information that must be contained in the application for disclosure, which includes the identity of the police officer applying for the direction and the description of the data which is sought.

Finally, section 44(9) provides for sanctions for failure to comply with the disclosure of data direction or for the making of false statements. Anyone found guilty will face a fine or imprisonment for a period not exceeding two years or both.[73]

5.4 Summation

The Budapest Convention and the Cybercrimes Act deal with international co-operation in similar terms. The Cybercrimes Act supports international co-operation by directing one to the International Co-operation in Criminal Matters Act so as to not burden itself with re-creating law which already exists. It does not pronounce much on the question of extradition, for example.

Whilst both the Budapest Convention and the Cybercrimes Act apply the territorial principle to jurisdiction, the Cybercrimes Act grants South African courts quite a wide scope which regard to how it will exercise jurisdiction. Notably, it does not give too much credence to the principle of dual criminality, electing rather to cast a wide net regarding the kinds of offences which may be prosecuted. This wide scope, however, is not without bounds, as certain decisions to exercise jurisdiction will have to be authorised by the National Director

71 The provisions in question are section 4(3) of the Customs and Excise Act, 1964; sections 69(2)(b) and section 71 of the Tax Administration Act, 2011; and section 21(e) and (f) of the Customs Control Act, 2014.

72 Section 44(a)(b) of the Cybercrimes Act

73 Section 44(9) of the Cybercrimes Act.

of Public Prosecutions. This is a necessary safeguard, especially for the maintenance of good diplomatic relations.

However, some of the other checks and balances can be rather cumbersome. An example is the unnecessarily long chain of command for requesting mutual assistance. This arrangement might be counterproductive in the long-run because of the fast-changing and volatile nature of cybercrime. It runs the risk of overburdening all of the offices involved in the process of approving requests and surely will cause unnecessary and undesirable delays.

Nevertheless, the Cybercrimes Act evidences a good grasp of what is necessary to ensure that offences do not go unpunished and that territorial borders are not a hindrance to the attainment of justice. The true test will be in how the various entities tasked with these responsibilities are able to implement the prescribed procedures.

CHAPTER SIX

THE CAPABLE GUARDIAN

6.1 Introduction

The focus of this chapter is upon the third and final constitutive element of the Routine Activities Theory (RAT), namely, the capable guardian. As previously mentioned, RAT posits that in order for there to be a successful commission of a crime, the motivated offender and the suitable target need to converge in time and space where a capable guardian is absent. The motivated offender was discussed in Chapter Three in the context of Type I cybercrimes, and the suitable target was discussed in Chapter Four in the context of Type II cybercrimes.

This chapter discusses the capable guardian as the necessary element that will protect the suitable target from the motivated offender. It does this by examining what a capable guardian is and how the concept has developed since being coined by the creators of RAT, Cohen and Felson, in 1979. It then discusses what a capable guardian in cyberspace would entail. It suggests a re-imagining of the concept of the capable guardian from its original form to what this study calls the *cyber capable guardian*. It argues that in order to combat cybercrime successfully, it is necessary to introduce artificial intelligence (AI) technology in the form of machine learning to create a cyber capable guardian which will perform functions that a human capable guardian would not be able to perform. Finally, it discusses section 52 of the Cybercrimes Act, which provides for the Designated Point of Contact (DPoC). It argues that the DPoC would be a suitable capable guardian if it were to be created as an independent agency which is incorporated as a private company in terms of the Companies Act 71 of 2008. It further argues that the DPoC should be established with the chief mandate of combating cybercrime through the creation and operation of the cyber capable guardian.

6.2 The Human Capable Guardian

In his later writings, Felson argued that in the explanation of crime, it is not necessarily the motivated offender who is the most important actor and that the capable guardian could

play the central role in crime and crime prevention.[1] When the capable guardian was introduced as a concept, it was defined as someone who prevents a crime from occurring by being present at a particular place at a particular time. The capable guardian was not conceptualised as a title that one assumes by virtue of an official position, but rather as a person who, by mere circumstance, is at the right place at the right time.[2] This means that although a police officer may be a capable guardian, a capable guardian need not be a police officer. The idea is that while police officers are able to prevent crimes, they are not always present at the scene of a potential crime to allow them to prevent it. It is more likely that a bystander is at the scene of a potential crime when the motivated offender is about to commit it.[3] Furthermore, one may be a capable guardian even without knowing that one is acting in that capacity. For example, a capable guardian may be a retired person who is at home during the day, thereby preventing a motivated offender from burglarising her home or her neighbour's home. It may be the case also that two people walking together in the street can deter a motivated offender from robbing them, because they unintentionally act as capable guardians for each other simply by being in each other's presence.[4]

RAT has developed substantially since it was formulated by Cohen and Felson in 1979. In comparison to the motivated offender and the suitable target, the capable guardian is considerably under-researched.[5] When Felson reconsidered the capable guardian in his later works, he defined the guardian as someone who keeps an eye on the potential target of a crime.[6] This suggests a level of awareness on the part of the capable guardian that she has some kind of responsibility towards the suitable target, albeit not necessarily a formalised responsibility. What underlined Felson's work was the idea of monitoring, which means that in order for the motivated offender to be deterred from committing an offence, there should exist an environment which suggests that there is someone who is watching and could detect untoward behaviour at any given moment.[7]

1 Felson (1995) at 53.
2 Felson (1995) at 53.
3 Felson (1980) at 53.
4 Felson (1995) at 53.
5 Hollis-Peele *et al* (2001) at 54.
6 Felson (1995) at 53.
7 Hollis-Peele *et al* (2001) at 55.

A major development of RAT as regards the capable guardian is the link that was drawn between it and Hirschi's control theory.[8] In essence, this link expanded the scope of the capable guardian by adding another layer to the concept. The control theory introduced the idea of attaching "handles" to motivated offenders or would-be offenders through established social bonds.[9] These handles then would become instruments of informal control of the motivated offender to prevent her from offending against the suitable target in the first place. This means that the role of the traditional capable guardian is taken over by the handler, who has a social responsibility towards the offender, not the suitable target.[10]

Thus, when considering the behaviour of young people in a community, the first level of handlers would be their parents because of their proximity to the young people and their intimate knowledge of youth behaviour.[11] The second level of social control would be the members of the community to which the offender belongs. They are familiar with the young people and "handle" them when they are within the community but outside the care of their primary handlers.[12] Take, for example, the relationship between a mother, a child, and the child's teacher. When a mother teaches her child to respect her elders or obey authority, she, as the primary handler, attaches handles to the child in the form of values. When the child goes to school, the responsibility for social control of the child is transferred to the teacher, the secondary handler. In order to exercise her power as a secondary handler, the teacher does not need to teach the child new values. Instead, she simply needs to grasp the handles (respect your elders, obey authority, and the like) created by the primary handler to enforce social control. The teacher merely has to say to the child: "Do not talk back to me. Remember that your mother taught you to respect your elders." Thus, social control is maintained outside the home by the community.

In short, informal social control requires attaching handles to youth on the primary level and then organising community life in such a way that handles may be grasped on the secondary level by the secondary handlers, such as neighbours, teachers and sports

8 Hirschi (1969); Gottfredson & Hirschi (1990).
9 Felson (2014) at 121.
10 Hollis-Peele et al (2001) at 57; Grasmick et al (1993).
11 Costello & Laub (2020) at 29.
12 Costello & Laub (2020) at 29.

coaches.[13] Thus, social control is dependent on keeping the suitable target near the capable guardian and the motivated offender near the handler. In both cases, direct physical contact plays an important role in discouraging criminal conduct. [14]

Eck has extended the control theory to include the control or monitoring of places.[15] Eck's study was conducted in the context of illegal drug markets. He argued that in the spatial structures of crime, there is a need for the inclusion of "managers" who are responsible for looking after places. A manager can be anyone, such as a homeowner, a receptionist, a doorman, a concierge, a close neighbour and a private security guard. Each of these people is a subset of the capable guardians and could serve to discourage the commission of crimes by looking after places.[16]

Therefore, the successful commission of a crime will occur when an offender, who is free from her intimate handlers, finds a suitable target unprotected by a capable guardian in a place which does not have managers. Collectively, the capable guardian, the handlers and the managers are referred to as controllers, and each of them may intervene to prevent the commission of a crime.[17]

These controllers are very useful for terrestrial crimes, because of the obvious direct physical contact with the motivated offender and the suitable target. However, they do not translate easily into cyberspace. They are worth noting because their formulation displays a willingness to develop the ambit of the capable guardian to accommodate the ever-changing landscape of crime. Felson embraced this evolution, which founds the efforts made below to develop the concept of the capable guardian further to cater for the challenges of cybercrime.

6.3 The Cyber Capable Guardian

Despite the developments regarding the capable guardian, when it comes to cybercrimes there is a clear reluctance to re-imagine the capable guardian as *something* rather than *someone*. In other words, there is an insistence that the capable guardian has to be a human

13 Felson (1995) at 54.
14 Felson (1995) at 54.
15 Eck (1994).
16 Felson (1995) at 54.
17 Felson (1995) at 55.

being who either is seen by the motivated offender or who implants the idea in the mind of the motivated offender that she is being watched at any given time. As a result, the trend has been towards what is referred to commonly as target hardening.[18]

Target hardening applies where the suitable target bears the responsibility for preventing perpetration of the offence.[19] Although some argue that the capable guardian is the most viable tenet of RAT to control the level of computer-crime victimisation,[20] the consensus is that target hardening significantly decreases risks of computer victimisation, such as cyber stalking and other forms of online harassment.[21] In computer security, the idea is to make it more difficult for the motivated offender to commit cybercrimes by updating and maintaining computer security, such as anti-virus software.[22] Some examples of target hardening against online victimisation include having adequate security software with appropriate filters, being proficient and skilled in computers and "online hygiene", and reducing risky information sharing.[23]

Target hardening is a very useful strategy against victimisation online. However, it must not be taken as a replacement for capable guardianship. This is because suitable targets are inherently vulnerable. If they always were able to protect themselves, there would be no need for this discussion. Furthermore, although some people may have the means to harden themselves as targets of terrestrial crime by installing alarm systems and high walls, this has not rendered police officers obsolete. Instead, what is needed is a reconceptualisation of the capable guardian, in line with technological advancement, to a kind of cyber capable guardian.

The cyber capable guardian needs to encapsulate the essence of the capable guardian but with a futuristic outlook. Traditionally, a capable guardian is someone who prevents the commission of a crime by converging in space and time with the motivated offender and the suitable target. Considering that only Type I cybercrimes may be considered true cybercrimes, as previously argued, the cyber capable guardian must be

18 Hollis-Peele *et al* (2001) at 54.
19 Johnson et al (2017) at 506.
20 Choi (2008) at 312.
21 Reyns *et al* (2016) at 154.
22 Choi (2008) at 312.
23 Reyns *et al* (2016) at 154.

designed in such a way that it addresses the challenges which are specific to Type I cybercrimes. The constitutive elements of a cyber capable guardian are considered below.

6.3.1 Big Data

Big data has become a buzz word in recent years. It is a composite term which describes the emerging technological capabilities for solving complex problems. It is hailed as a new frontier for innovation, competition and productivity. Big data is multifaceted, multidimensional and multidisciplinary, finding application in various industries such as health, science, technology, transport and cybersecurity.[24]

Each day billions of individual pieces of data are being amassed from various sources, including supplier data, delivery slips, employment records, health records, police criminal databases, DNA records, and user-generated content such as check-in locations, messages, photos and videos on social media platforms. The availability of big data contributes to motivating researchers from diverse fields — ranging across physics, computer science, genomics and economics — not only to investigate new methods and algorithms for detecting and sorting chunks of big data but also to invent them. Analysing more data faster can lead to better and more efficient decisions in areas such as finance, health and research.[25]

There is still a lack of consensus on a single definition of big data, but it is clear, from the different areas where it is applicable, that there are common characteristics. The International Telecommunications Union (ITU) refers to the four Vs which often are used to characterise different aspects of big data. They are volume, velocity, variety and veracity.

Volume — the first V — refers to the issue of data anytime, anywhere, of anything and by anyone. One of the most attractive things about big data is volume. The statistics differ but it is estimated that more than 90 per cent of the data in the world was created in the past decade, with both machines and humans contributing to the data growth.[26] It is not specified how much data would count as big or big enough. Network manufacturer Ericsson envisions that more than 50 billion devices will be connected by the year 2020, as

24 Oussous et al. (2018) at 432.
25 Oussous et al. (2018) at 436.
26 ITU (2013) at 8.

ubiquitous broadband connectivity is a major driver of data volume as well as data variety.[27] ITU estimates that there are almost seven billion mobile-cellular subscriptions worldwide which both consume and create data. The volumes of data created grow at a tremendous rate. The *Exabyte era* (10^{18} bytes or over 36 000 years' worth of high definition (HD) videos) has been superseded by the *Zettabyte era* (10^{21} bytes or a trillion gigabytes). We are told that it is merely a matter of time before we see the dawn of the *Yottabyte* (10^{24} bytes).[28]

Velocity — the second V — refers to the notion that every millisecond counts. A critical factor in the big data discussion is the speed of decision-making, that is, the time that elapses between the data input and the decision output. This involves the need for data processing capabilities for vast volumes of data which should occur in real- or near real-time.[29] Emerging technologies are gaining those capabilities, thereby aiding organisations to respond appropriately to changes in the field. Furthermore, not only should data systems have processing capabilities, they also should be able to handle data and draw links and patterns from it. An example of this may be gleaned from how data is used in the day trading practices of stock exchanges. The race for data velocity and tight feedback loops plays a key part in giving an organisation a competitive advantage in a number of industries.[30]

Variety — the third V — refers to the reality that data is messy. Big data encompasses all kinds and structures of data, including text, sensor data, call records, maps, audio and visual information.[31] A vast majority (estimated at 80%) of all data is said to be unstructured as it can present in many different forms, such as emails, call logger data and social media feeds. The term unstructured data refers to the fact that there is no latent meaning that is attached to the data in a way that a computer can understand. By contrast, structured data has a semantic meaning. For example, a database contains data that is represented by means of rows and columns which can be understood immediately by a

27 Galetic (2011) at 384. At the time of writing, the official estimates for 2020 had not yet been determined. However, in its November 2019 quarterly report, Ericsson recorded that the number of mobile subscriptions globally was 8 billion with 10.8 billion Internet of Things (IoT) connections globally. See Ericsson Mobility Report (2019) at 4 & 17.

28 ITU (2013) at 11.

29 ITU (2013) at 8.

30 ITU (2013) at 8.

31 ITU (2013) at 8.

computer system and may be transformed to be of interest to end-users, for example, Microsoft Excel spreadsheets.[32] An example of unstructured data would be a set of alpha-numeric characters on a document which do not have a decipherable pattern and which do not have a programme which can discern their meaning, that is, an encrypted message without a decryption key. Structured data is easier to handle because there is more information available to a programme to enable it to determine what the data means.

Veracity — the final V — refers to the accuracy of the data upon which decisions will be based. Some data may be more reliable than others, for example, statistics from a research centre data as opposed to unverifiable statistics on a tweet. Veracity is influenced by the three other Vs and it can be uncertain because of many inconsistencies, incompletenesses, ambiguities and latencies. Poor quality data is costly and so it is essential that programmes are capable of distinguishing, evaluating and weighing different datasets so that veracity can be maintained.[33]

Veracity is linked closely to the acronym GIGO which stands for "garbage in, garbage out". GIGO is premised on the idea that, regardless of how good the system or programme is, if the input data is garbage, the output decision will be garbage also. In this case, there may even be instances where big data is simply not big enough to yield accurate results, as in a case where a sample size is simply too small to draw meaningful conclusions. Another challenge with big data is that the system or programme may not have the necessary mechanism in place to detect what data is garbage, which may lead to the perpetuation of garbage data outputs.[34] In order to gain insights and knowledge from big data, it is essential that the dots are connected by aggregating and analysing the data so that patterns may be detected and accurate, comprehensive and actionable reports may be produced.[35]

Some of the challenges of big data relate to data protection, privacy and cybersecurity. Two main principles of data protection are data minimisation and data avoidance, which are in stark contrast to what big data represents. Big data can keep track of people's behavioural patterns with incredible accuracy and often without consent. This is of great concern for personal privacy when abused, but when done properly and legally it

32 ITU (2013) at 9.
33 ITU (2013) at 8.
34 Clegg (2017) at 28.
35 ITU (2013) at 1.

can be a great source of information for an entity such as the cyber capable guardian. For instance, large sets of phone call records or data traffic over the internet, even if anonymised and stripped of all personal information, can be used to identify individuals and create a highly accurate profile or "fingerprint" of users. Such a fingerprint, when used in combination with geo-location data, can be very helpful to an investigator.[36]

Internet services providers (discussed in §6.3.2 below) are typically good sources of big data, either as creators or as users. The relationship between big data, internet service providers and capable guardians is of cardinal significance because it is where some of the challenges of investigating and prosecuting cybercrimes begin to be solved.

6.3.2 Internet Service Providers

Victims and perpetrators of cybercrime correctly are central to discussions on prevention because it affects them directly. Regrettably, however, significant third parties, such as internet service providers (ISPs), usually are left on the fringes even though they play a key role in combating cybercrime.

ISPs are businesses or non-profit organisations providing specific services which are essential to the operation of the internet. Their main function is to store and transmit internet traffic. They encompass hosting providers (which host websites and make the content available through the internet), access providers (which provide end-users with internet access), and other content and service providers, such as search engines, trading platforms and social media.[37]

The first line of defence against cybercrime is to take preventive measures. ISPs are placed uniquely to detect and block malware that is transmitted via internet traffic. Take, for instance, a DDoS attack being carried out by a botnet. If the ISP is able to distinguish a

36 ITU (2013) at 16.

37 Tjong *et al* (2015) at 26.
Article 1 of the Budapest Convention defines a service provider as a public or private entity that enables its users to communicate through a computer system. The Cybercrimes Act does not refer to ISPs but instead speaks of an electronic communications services provider which is defined to mean "any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No 36 of 2005), or who was deemed to be licenced or exempted from being licenced as such in terms of the Electronic Communications Act, 2005".

botnet communication from a legitimate communication, it could interrupt the communication before it causes harm to the suitable target.[38] A botnet may be detected by the particularities in its network behaviour. If, for example, large amounts of spam are sent out via a botnet, the ISP of the botnet client may become aware of the spam and determine which of the ISP's customers may have been infected by malware. The ISP is in a position either to warn its customer or even to block the customer's internet in an effort to encourage the customer to clean her computer or instal stronger security measures. Another technique that ISPs may use is blacklisting. This is where an organisation keeps a list of suspicious or untrusted IP addresses and/or domains which may be accessed by subscribers to that list so that they can refuse to allow traffic to and from the blacklisted addresses. This is similar to the way in which large search engines, such as Google, flag suspicious websites and refuse to make a connection.[39]

The same is true of ransomware attacks. If an ISP is informed about a ransomware attack or infection, it could help in tracing the source of the ransomware. However, this is dependent on whether it bears a legal obligation to assist in finding the motivated offender behind the attack. In many cases, ISPs are not obligated thus.[40] If ISPs have a duty of care when it comes to cybercrime, they could be instrumental in detecting malicious activity, detecting network patterns of botnets, blacklisting websites, filtering spam, warning end-users of infections, and providing assistance to law enforcement.[41] There are relatively few international norms which impose a duty of care and diligence on ISPs in relation to cybercrime.

38 Tjong *et al* (2015) at 43.
39 Tjong *et al* (2015) at 44.
40 Tjong *et al* (2015) at 47.
41 Tjong *et al* (2015) at 49.

One norm that does do so is the E-Commerce Directive 2000/31/EC, which exempts an ISP from liability for the information which was transmitted or hosted, as long as the ISP remained passive in respect to the information.[42]

The Budapest Convention recognises that the interception of content data is a very intrusive measure which warrants stringent safeguards being taken by States Parties to ensure that the appropriate balance is struck between the interests of justice and fundamental rights. The Convention itself does not set out specific safeguards, other than limiting the authorisation of interception to serious criminal offences as defined by the domestic criminal law. Some of the safeguards include judicial or other independent supervision, necessity, subsidiarity and proportionality, limitation on the duration of the interception, and right of redress.[43] The quest for cybersecurity has to be balanced against the protection of fundamental rights. This means that even where ISPs are able to aid in counteracting certain cybercrimes, they may be limited by the need to respect certain fundamental rights, such as privacy and the right to access and share information.

The ability of ISPs to monitor networks is not without its challenges. One of the more prominent issues is the concept of *net neutrality* which requires that ISPs treat all internet traffic equally. This means that an ISP may not block or otherwise hinder the transmission of content. ISPs are forbidden by public law to discriminate between various forms of content. Once an ISP starts actively to participate in network monitoring, it no longer may qualify for exemptions against liability because it would no longer be passive.[44]

---

42 Article 42 of the Directive provides that the exemptions from liability established under it cover only cases where the activity of the service provider is limited to the technical processes of operating and giving access to a communication network. This means that it extends only to activity which is of a mere technical nature such as where it transmits or stores temporarily the information of a third party. The service provider's sole purpose should be to make the transmission more efficient. Ideally, in an automatic and passive manner so that it has neither knowledge of nor control over the information which is being transmitted or stored.
Article 43 provides further that a service provider can only benefit from the exemption for being a mere conduit or for caching if it does not modify the transmissions in any way. This requirement, however, does not cover manipulations of a technical nature which inevitably may occur during transmission, so long as the integrity of the information is not compromised.
Finally, Article 44 provides that a where a service provider deliberately collaborates with one of the recipients of its service in order to participate in illegal acts, it can no longer benefit from the liability exemptions as that conduct would no longer count as being a mere conduit nor as caching.

43 Budapest Convention, Explanatory Report at 37.

44 Tjong *et al* (2015) at 159.

For instance, in the case of a DDoS attack, an ISP understandably would be expected to delay all requests sent to the website server which is under attack. However, it is possible that some of those requests stem from *bona fide* users. This means that if an ISP is too active in delaying communication from suspected malware, it runs the risk of being accused of discriminating against a legitimate application. This puts the ISP at risk of incurring hefty fines for violating net neutrality.[45]

The reality is that even though ISPs may be placed uniquely to address cybercrime challenges, they also are placed in a precarious position because they risk running foul of applicable norms and of violating fundamental rights. However, this should not be misunderstood to mean that their hands are tied. What is required is a determination of the parameters within which they may act.

6.3.3 Interception of Data by Law Enforcement

The Cybercrimes Act does not have a dedicated provision for interception because South Africa has enacted the thoroughly comprehensive Regulation of Interception and Provision of Communication-Related Information Act (RICA).[46] Similarly, the Act does not provide specifically for the collection of data. Nevertheless, for purposes of illustrating the critical role of ISPs, the concept will be considered through the provisions in the Budapest Convention.

There are two types of data which may be collected: traffic data and content data. Traffic data is defined in the Budapest Convention as:

> any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication,

45 Tjong *et al* (2015) at 159.

46 Act 70 of 2002. Conventionally, the interception of telecommunications refers to traditional telecommunications networks, such as cable infrastructures (for example, telephones), as well as to inter-connections with wireless networks (for example, cell phones). Computer communication networks may consist of fixed cable infrastructure, such as those that connect different countries via the ocean floors. More frequently, though, they are operated as virtual networks through telecommunications infrastructure, making them more global in nature. This has created a situation where there is a blurred distinction between traditional telecommunications networks and computer communication. Thus, it is not necessary to be pedantic about how a computer system is interconnected, in the sense that one need not concern oneself with how specific communications which are to be intercepted are transmitted from one computer system to the other. See the Budapest Convention, Explanatory Report at 35.

> indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.[47]

Content data is not defined formally, but refers to the meaning or purport of the communication or the message or the information, other than traffic data, being conveyed by the communication.[48]

Article 20(1)(a) of the Budapest Convention obligates Parties to ensure that their competent authorities have the capacity to collect and record traffic data by technical means. Article 20(1)(b) requires Parties to ensure that their competent authorities have the power to compel ISPs to collect or record traffic data or compel them to co-operate with the authorities. This obligation applies to the extent that the ISPs have the capacity to collect or record traffic data. In other words, competent authorities should not compel ISPs to reconfigure their systems, acquire or develop new equipment or hire expert support. It is only if the ISPs have the capacity already that they are obligated to act.[49] The measures provided for in Article 20(1)(a) and Article 20(1)(b) are not alternatives, meaning that both collection routes may be used, because if the ISP does not have the requisite capabilities, the competent authority should.

Real-time collection of traffic data is an essential part of cybercrime investigation because historical traffic data may no longer be available or may be rendered irrelevant if the offender has changed the route of the communication. Given that computer technology is capable of transmitting vast quantities of data, it presents ready opportunities for the commission of crimes. Thus, it is necessary to collect data in real time because it reduces the window of opportunity for motivated offenders to interfere with the integrity of data, which carries with it a great potential for economic, social or personal harm to occur.[50] Furthermore, major damage to the proper operation of computer systems can occur if there is any interference with the data which relates to key operational functions. Law enforcement must be capable of tracing the route of communications back from the victim to the offender. The correlation of time, data, source and destination of the offender's communications with the time of the intrusions into the computer system of the victim is

47 Article 1(d) of the Budapest Convention.
48 Budapest Convention, Explanatory Report at 35.
49 Budapest Convention, Explanatory Report at 38.
50 Budapest Convention, Explanatory Report at 37.

vital. The ability to collect traffic data in respect of communications is just as important, if not more so, as collecting evidence from traditional telecommunications, such as the details of telephone conversations.[51]

Modern insights into regulations and governance recognise that the ability to combat cybercrime may depend on a combination of diverse forms of regulation and enforcement. The public and private sectors may need to work in tandem.[52] The nature of cybercrime may necessitate heavy reliance upon the private sector, and upon ISPs in particular. This may be observed from Title 5 of the Budapest Convention, which makes provision for real-time collection of computer data. Articles 20 and 21 provide for the collection of traffic data and for the interception of content data respectively. In both articles, the Convention stipulates that Parties should adopt legislative and other measures needed to empower their competent authorities to collect content data themselves or to compel service providers, who have the means, to co-operate and assist in the exercise. It is clear from these provisions that public-private co-operation not only is envisioned, but also is enforced in respect of certain service providers.

Articles 20 and 21 of the Budapest Convention do not make a distinction between publicly- and privately-owned telecommunications or computer systems. Therefore, even if a Party were to draw a public-private distinction, the provisions of the Convention would apply equally to both.

6.3.4 Artificial Intelligence and Machine Learning

Type I cybercrimes are technical in nature, which means that the spatio-temporal convergence will occur in cyberspace and not in the terrestrial realm. It may be extrapolated herefrom that a guardian who truly is capable of disrupting the commission of a cybercrime is one who is able to operate predominantly in cyberspace, that is, a cyber capable guardian. It follows also that the proposed cyber capable guardian cannot be a human being. It will have to be a machine. Additionally, given the rate at which Type I cybercrimes develop, the machine-guardian must possess qualities which would allow it to adapt rapidly and without human intervention to any new and emerging threats. It should have a kind of *intuition* or

51 Budapest Convention, Explanatory Report at 37.
52 Tjong *et al* (2015) at 13.

intelligence that a human would have, while being endowed with the superior technical capabilities of a machine. In other words, the proposed cyber capable guardian ought to be a machine based on the technology of artificial intelligence (AI).[53]

Artificial intelligence is still a relatively new field in the cyber world, with promising research being conducted in a host of areas. One of the aspects of AI which already has found many uses is machine learning. Machine learning is a result of the intersection between computer science and statistics.[54] While machine learning builds upon the issues raised by computer science and statistics, it pursues its own distinct concerns about how to enable computers to programme themselves from experience and initial structure.[55] Machine learning is a field of knowledge which attempts to answer the question, "How can we build computer systems that automatically improve with experience, and what are the fundamental laws that govern all learning processes?"[56]

There is a broad range of learning tasks covered by this question. It includes the tasks of how to design autonomous mobile robots which would be able to navigate from their own experiences. It includes also learning tasks such as data mining, autonomous discovery, database updating, and programming by example.[57] Machine learning is special in that it can be applied to many different fields, from the study of human and animal learning in psychology and neuroscience to information security and data mining.[58] The flexibility of machine learning means that it may be applied to law in the fight against cybercrime, particularly because technology is the backbone of cybercrime.

Machine learning uses data to learn programmes automatically. This is an attractive capability, because it reduces the burden of having to construct programmes manually. Tasks related to cybercrime in which machine learning is used include web search optimisation, recommender systems, advertisement placement, credit scoring, fraud

53 Russell & Norvig (2016).
54 Mitchell (2006) at 1.
55 Oussous (2018) at 435
56 Mitchell (2006) at 1.
57 Mitchell (2006) at 1; Oussous (2018) at 434.
58 Mitchell (2006) at 1; Oussous (2018) at 434.

detection, stock trading and drug design. It is anticipated that machine learning will be the driver of the next wave of digital innovation.[59]

One of the areas in cybercrime where machine learning has been applied relatively successfully is in spam detection. Email clients and social networking platforms experience many challenges with spam.[60] Spammers have used social networking platforms, such as Twitter, as a tool to post unsolicited messages to users, to spread malicious links and to hijack trending topics.[61] Twitter responded by employing target hardening techniques to combat the proliferation of spam. It did this by soliciting the users of the service to participate in detecting and identifying spam by adding a "report as spam" feature to the service. This was aimed at cleaning up accounts which were considered to be suspicious. Most recently, it cut down the number of accounts one can follow in a day from 1000 to 400.[62]

It is apparent from the above discussion that great strides have been made in machine learning technology. Indeed, the extent of the capabilities of machine learning is being discovered still. Governments need to invest in research into machine learning and, it is submitted, must facilitate the construction of machines which will take on the role of a cyber capable guardian. It is here where big data would play its biggest role. It is essential that when developing the cyber capable guardian, sufficient safeguards are put in place to ensure that the data which is being fed to the AI is not garbage.

The elements identified in the preceding discussion are the essential building blocks of the cyber capable guardian which will be discussed shortly. As already noted, in order for the capable guardian to be effective, it needs to operate predominantly in cyberspace. This can be achieved only if it takes advantage of some of the resources that ISPs have, which include access to big data to create and run machine learning technology.

Each of these elements plays a big and important role in the fight against cybercrime, but it must be borne in mind that in order to be a successful custodian of the cyber capable guardian, a multi-disciplinary and multi-party approach must be adopted. This

59 Domingos (2012) at 78.
60 Graham & Triplett (2016) at 10.
61 Wang (2010) at 335; El-Mawass et al (2018) at 7.
62 Perez (2019) at 1.

means that the fight against cybercrime should not be viewed through a myopic lens. In other words, combating cybercrime cannot be seen only as a policing or criminal justice issue. Other disciplines, such as engineering and computer science, have to be factored in. Innovation is key.

6.4 The Capable Guardian and the Cybercrimes Act

Article 35 of the Budapest Convention provides for the 24/7 network. It requires each Party to designate a point of contact, which must be available 24 hours a day and seven days a week, in order to ensure that there is immediate assistance available for the purpose of investigations or criminal proceedings related to cybercrime. Such assistance must include the facilitation or, if permitted by the domestic law, the direct provision of technical advice, the direct preservation of data in terms of Articles 29 and 30, and the direct collection of evidence, supply of legal information and locating of suspects.[63]

The point of contact of one Party is required to have the capacity to carry out communications with the point of contact of another Party.[64] If the designated point of contact is not responsible itself for international mutual assistance or extradition, it must ensure that it is able to co-ordinate with the responsible authority on an expedited basis.[65] With reference to the discussion of mutual assistance and international co-operation in §5.3 above, having the cyber capable guardian function at optimal level is to the benefit not only of South Africa but also to the states which will seek mutual assistance from South Africa. One might say even that it is a country's implied duty to ensure the highest level of efficiency for the cyber capable guardian, even if the Convention itself does not impose this duty. The anti-cybercrime chain is only as strong as its weakest state.

The 24/7 network is based on the experience gained from the functioning of the network which already exists and operates under the auspices of the G8 group of nations. The G8 24/7 Cybercrime Network was created in December 1997. This Network consists of more than 70 countries, including South Africa. It exists primarily to preserve digital

63 Article 35(1) of the Budapest Convention.
64 Article 35(2)(a) of the Budapest Convention.
65 Article 35(2) of the Budapest Convention.

evidence which will be transferred subsequently through legal channels.[66] It was agreed amongst the members that the establishment of the Network is one of the most important means of ensuring the effective and rapid response of law enforcement to cybercrime for which the Convention has provided.[67]

The Protocol statement of the G8 24/7 Cybercrime Network recognises that high-tech crimes pose new challenges to law enforcement and hence it is imperative that technically literate investigators be capable of moving at unprecedented speeds to preserve electronic evidence and locate suspects during investigations, often by asking ISPs to preserve data. The G8 Network was created, therefore, to enhance and supplement (but not to replace) traditional methods of obtaining assistance. It was established as a new mechanism for the expedition of contacts between the participating Parties and any other autonomous law enforcement agencies.[68]

In order for a state to become party to this Network, it must have: (a) a 24/7 point of contact; (b) an English-speaking contact point; (c) a technically knowledgeable contact point; and (d) a contact point who is knowledgeable about domestic law.[69] Although the number of requests which have been made through this Network thus far have been relatively low, it has been shown to be beneficial as a crime-fighting route, as seen in the $10 million Norwegian bank robbery during which a police officer was shot dead. The Norwegian police used the Network to request the preservation of computer data from the UK, an effort which led to Norway's most wanted suspect being traced to an internet café in Spain, where he was apprehended by the Spanish Police.[70]

Section 52 of the Cybercrimes Act is dedicated to the establishment of the Designated Point of Contact (DPoC), previously known as the 24/7 Point of Contact in version [B6—2017], which reflected the idea that the point of contact would have had to operate for 24 hours a day and seven days a week. This approach was informed by an acknowledgment that, because of the nature of the internet, cybercrime necessitates round-the-clock monitoring. Thus, despite the change of the name, the DPoC retains the

66 Ott (2018) at 1.
67 Budapest Convention, Explanatory Report at 54.
68 Organisation of American States (undated) at 1.
69 Organisation of American States (undated) at 1.
70 Organisation of American States (undated) at 1.

function of its predecessor, to provide non-stop vigilance against and assistance with cybercrime.

The South African National Police Commissioner is responsible for the administration and functioning of the DPoC, which must be designated to ensure that immediate and expedited assistance is available.[71] The services to be provided by the DPoC include: technical advice and assistance regarding cybercrime; anything which is authorised under Chapter 4 (powers to investigate, search and access or seize) and Chapter 5 (mutual assistance) of the Cybercrimes Act; legal assistance; the identification and location of an article;[72] the identification and location of a suspect; and co-operation with the appropriate authorities of foreign states.[73] The DPoC is meant to assist also in proceedings or investigations regarding the commission or intended commission of any of the offences provided for in the Cybercrimes Act. In addition to this, the DPoC will exercise power over any other crimes which may be similar to these or any crimes which may be facilitated by means of an article.[74] Further, section 52 provides for an international dimension by catering for offences committed in a foreign state but which are substantially similar to those described in the Cybercrimes Act.[75]

The NDPP must avail members of the National Prosecuting Authority (NPA) to provide legal assistance to the DPoC, with a view to making it as effective as possible.[76] Such members of the NPA must have particular knowledge and skills in respect of any matter dealt with in the Cybercrimes Act. Also, they must possess the necessary security clearance as issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994.[77]

---

71 Explanatory Note 63 (Version [B6—2017] of the Cybercrimes Act).

72 In section 1 of the Cybercrimes Act, the word "article" is defined as any data, computer programme, computer data storage medium or computer system which (a) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission of a crime; (b) may afford evidence of the commission or suspected commission; or (c) is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission of an offence in terms of chapter 2 or section 17, 18, or 19 or any other offence which may be committed by means of or facilitated through the use of such article, whether within the Republic or elsewhere.

73 Cybercrimes Bill [B6—2017], Explanatory Note 63of the.

74 Section 52(3)(ii) of the Cybercrimes Act.

75 Section 52(3)(iii)(bb) of the Cybercrimes Act.

76 Cybercrimes Bill [B6—2017], Explanatory Note 64.

77 Act 39 of 1994.

The Minister of Police will be entitled to make regulations for any matters related to the DPoC.[78] Said Minister will be required also to submit a report on the functions and activities of the DPoC to the Chairperson of the Joint Standing Committee on Intelligence at the end of each financial year. This report must include the number of matters in which technical advice and assistance were provided to a foreign state and the number of matters in which technical advice and assistance were received from a foreign state.[79]

Finally, the DPoC is to be established or designated by the National Police Commissioner within the existing structures of the South African Police Service (SAPS).[80] There well may be good reasons for housing the DPoC in the existing structures of SAPS, such as the Cybercrimes Unit. Unfortunately, the Cybercrimes Unit appears to be beset with its own challenges. In September 2018, it was reported that SAPS had ceased investigation of thousands of cases because certain software licences had lapsed due to non-payment. The deferred investigations included investigations into hacking, EFT scams and organised crime, which had to be halted because the software that is used to interpret cell-phone data had expired.[81] This is undoubtedly problematic.

Whereas it may appear feasible to locate the DPoC within SAPS, it may have more chance of success as a capable guardian against cybercrime were it to be established as an independent agency along the lines of the State Information Technology Agency (SITA), as established by the State Information Technology Agency Act (SITA Act).[82]

SITA is the lead information technology agency for the South African state. It provides relevant ICT products, services and solutions to the government. It aims to:

> leverage economies of scale to cost effectively procure IT goods and services and to set standards for security and interoperability in government implementation of core ICT programmes.[83]

The SITA Act established a juristic person, called SITA, which is incorporated as a private company in terms of the Companies Act. The state is the sole shareholder in SITA, and it resorts under the authority of the Minister of Public Services and Administration or anyone

78 Section 52(4) of the Cybercrimes Act.
79 Section 52(6) of the Cybercrimes Act
80 Section 52(1) of the Cybercrimes Act.
81 MyBroadband (2018) at 1.
82 Act 18 of 1998.
83 SITA at 1.

appointed by the President. When SITA was created, it comprised the Central Computer Services of the Department of State Expenditure, Infoplan, the sub-component Information Systems within the Department of Safety and Security, and any other department approved by the Minister of Public Services and Administration.[84] In general, the provisions of the Companies Act apply to SITA, unless excluded by said Minister.[85]

SITA was created with the objective of providing information technology, information systems and related services in a maintained information systems security environment to, or on behalf of, participating departments and organs of state. It operates as an agent of the South African government.[86] It is governed and controlled by a Board of Directors which is appointed by the Minister of Public Services and Administration after consultation with Cabinet, and the Board approves the business and operational plans of SITA.[87] The Director of SITA must carry out her duties in accordance with the provisions of the SITA Act and the Companies Act.[88]

SITA is funded mostly by monies it receives from the services it renders to participating departments and organs of state. However, the capital required to start SITA is obtained from funds that are agreed upon by the Minister of Public Services and Administration and the Minister of Finance, after consultation with relevant participating departments. Where there is a need for special funding or any other special financial agreements, such as government grants, these must be negotiated by SITA with the Minister of Public Services and Administration and the Minister of Finance and any other interested party. SITA is allowed also to receive donations, which must be approved by the Minister of Public Services and Administration and recorded in the annual report of SITA.[89]

There are a number of benefits to having an independent and privately incorporated agency operating as a capable guardian. With this in mind, it is submitted that the DPoC prescribed by the Cybercrimes Act ought to be incorporated as an agency, in the same way as SITA has been, in which capacity it will act as the overarching capable guardian charged

84 Section 3(4) of the SITA Act, 1998.
85 Section 3(4) of the SITA Act, 1998.
86 Section 6 of the SITA Act, 1998.
87 Section 8 of the SITA Act, 1998.
88 Section 9 of the SITA Act, 1998.
89 Section 16 of the SITA Act, 1998.

with protecting the country against cybercrime. This submission means that this incarnation of the capable guardian will deviate from the traditional conceptualisation by not being embodied in a single natural person charged with the responsibility for preventing attacks on the suitable target.

The idea is that the DPoC will be in charge of the overall administrative functioning of the cyber capable guardian, which will be made up of the various machine learning instruments, networks and techniques. To employ an imperfect analogy, imagine the DPoC as a version of SAPS and the machine learning technology (in whatever form) as a version of the police officers who actually would fight crime. The higher-ranking police officers, such as the commissioner, the captains and the detectives, may be likened to the human engineers, software developers, IT specialists and technology experts who would be in charge of creating and running the machine learning complex. There needs to be a close relationship between work that is done by the machines and the humans in the DPoC in order to obtain the best results. It is understood well that although artificial intelligence and machine learning can perform actions that human beings cannot, human beings are not dispensable (at least not for now). Soft skills such as leadership, emotional intelligence and creativity remain the *forte* of humans still. Therefore, it is necessary to utilise both machines and humans to produce the best solutions.

As to the benefits (referred to above) of having an independent and privately incorporated agency operate as the capable guardian, the first is that the money that is allocated by the Minister of Finance to establish the DPoC will be dedicated to combating cybercrime. If the DPoC were part of SAPS, the discretion as to how to fund the office of the DPoC would be left to the National Police Commissioner. It is foreseeable that, given the challenges which accompany the rampant crime in South Africa, the priority would be to tackle terrestrial crime, such as murder and robbery, instead of cybercrime, which is not understood fully. If, however, the DPoC were incorporated as a private company in the same way as SITA is, it could use the money allocated to it to lay the foundation of an agency that can generate its own income. Unfortunately, the agency would not be able to raise funds by offering shares on the stock market, as do other corporations (given that government would be the sole shareholder), but it can participate in income-generating activities, such as providing services to both the public sector and the private sector. It can

be seen here how a mutually beneficial relationship between the DPoC and ISPs could be fostered.

The second benefit of an independent agency is that it would not be stifled by government bureaucracy. It would have the freedom to go about its business, such as entering into private contracts that generate income, unimpeded. This would mitigate the drawbacks of not issuing shares to corporations, while allowing the DPoC still to benefit from information and resource sharing. It would not be favourable for private companies to have shares in the agency because that could place it at the mercy of shareholders who want to further their own interests. It is important to remember that the ultimate goal of the DPoC would be to act as a cyber capable guardian for all of South Africa, and not to turn a profit.

The third benefit, similar to the second but from a different perspective, is that while the DPoC may be able to avoid government bureaucracy, it still would be subject to some government oversight and be involved in co-operation with other departments and entities, such as the NPA. Furthermore, it would be able to bridge the gap between the public and private sectors.

One of the provisions in version [B6—2017] of the Cybercrimes Bill, that was not retained in the latest version [B 6B—2017] and the Act, is section 55, titled “Nodal Points and Private Sector Computer Security Incident Response Teams”. That section contained provisions which would have been useful in fostering co-operation between government and the private sector. Section 55(1) mandated the Minister of Communications to declare that various sectors which provide electronic communications services are required to establish nodal points. These sectors would have been responsible for the establishment and operating costs of the nodal points. Where a designated sector failed to identify or establish a nodal point, then the Minister of Communications would have been allowed to identify and establish the nodal points as she deems fit, after engaging in consultations with the relevant sector.

Nodal points were intended to be structures which received and distributed information regarding cyber security incidents. The section in question also recognised private sector computer security response teams which would be expert groups that would handle cyber security incidents. Each nodal point would have been responsible for

distributing information regarding cyber incidents to the other sectors. It would have been responsible also for receiving and distributing information.[90]

Version [B6—2017] also catered for referring cyber security incidents to the Cybersecurity Hub, which would have been created under the now deleted section 55(4). The Cybersecurity Hub was aimed at promoting cyber security in the private sector. This body would have been an excellent supplement to the DPoC. Alternatively, it could have been subsumed under the DPoC in order to minimise costs relating to operating two bodies with similar mandates.

The fourth benefit of an independent agency is that when the cyber capable guardian is created, it may be customised from inception to cater for the needs of the country. The DPoC can engage in robust and dedicated research and development (R & D) in the same way that multinational corporations, like Google and Facebook, do. If the DPoC merely were incorporated into SAPS, there would be the temptation to apply existing crime fighting measures used by SAPS, which most likely would be outdated and ineffective in relation to cybercrime. The DPoC will have an opportunity to break the mould and ensure that the government invests in up-to-date and future-thinking technology which develops as fast as the technology that cybercriminals have at their disposal.

6.5 Summation

Whereas traditional ideas of controllers are useful for terrestrial crimes, cybercriminality requires innovation. RAT allows us to conceptualise clearly the life cycle of a crime. It tells us that the commission of a crime will occur when an offender, who is free from her intimate handlers, finds a suitable target unprotected by a capable guardian in a place which does not have managers. This understanding makes it relatively easy to figure out how to respond to cybercrime.

Hitherto, the responses to cybercrime have been dedicated, more or less, to target hardening, which shifts the focus from the motivated offender to the suitable target. Unfortunately, due to the fact that suitable targets are inherently vulnerable to victimisation, target hardening is not enough. While target hardening has been shown to

90 Section 55 of [B6—2017].

decrease risks of computer victimisation, a capable guardian remains indispensable. Furthermore, the technical nature of Type I cybercrimes necessitates the creation of a cyber capable guardian. While there are many instances of convergence between cyberspace and the "real world", each tends to face different challenges which require different responses. A machine learning cyber capable guardian can achieve what a human being cannot, especially if it co-operates effectively with ISPs.

The DPoC needs to be considered as an independent agency taking the role of capable guardian against cybercrime. As overall capable guardian, it would be in charge of the overall administrative operation of the cyber capable guardian. A dedicated and independent agency will have the autonomy to dictate the strategic allocation of resources, keeping in mind cybercrime trends. Additionally, it would not suffer from the bureaucratic nightmares that have been observed to cripple many existing government departments. Administrative freedom is essential for running a functional and effective agency. However, the model proposed here also benefits from a kind of government oversight which provides necessary accountability measures. This is important because the task of fighting crime is ultimately a government responsibility. Co-operation with the NPA, for example, would ensure that the justice exercise is carried through to completion. Finally, an independent DPoC would have the space to break the mould by investing heavily in research and design: a cyber capable guardian cannot come into existence otherwise.

CHAPTER SEVEN

CONCLUSION

7.1 The Cybercrimes Act

Cybercrime is a global threat which is becoming greater as the world advances technologically. Although Africa was the last continent to embrace ICTs, it has not been spared the explosion of cybercrime attacks. Regrettably, Africa is held back by the slow pace of technological development, particularly as regards telecommunications infrastructure. In addition, Africa experiences a dearth of policies and legislation which can address adequately the threats that come with cybercrime.

South Africa is no stranger to cybercrime and has seen its fair share of cybercrimes perpetrated against individuals, companies and other organisations, and even against the government itself. In 2015, Parliament responded by introducing the first comprehensive piece of legislation dealing directly with the challenge of cybercrime, in the form of the Cybercrimes Bill. The Bill has seen a number of versions, culminating in the Cybercrimes Act 19 of 2020.

The Cybercrimes Act came on the heels of South Africa's signing of the Council of Europe Convention on Cybercrime (Budapest Convention), even though it has not ratified said Convention yet. The Cybercrimes Act appears to have taken direction from the Convention, by catering for many of the offences that have been recommended by it. This means that the Act accords with international standards, norms and practices.

The chief aim of this study was to discuss the South African legislative response to cybercrime in the form of the Cybercrimes Act, and to determine whether the Act will be able to address the problem of cybercrime in South Africa. Having considered the Cybercrimes Act critically, the study came to the conclusion that it is an appropriate legislative response to cybercrime which, as a statute, ought to be effective in the fight against cybercrime.

The engagement with the Cybercrimes Act began by hypothesising that the problem of cybercrime is two-fold. It was asserted that the first problem with cybercrime is that its proliferation, both globally and in South Africa, is growing at a rate which outstrips the pace

at which governments are able to respond. The second problem is that where governments are able to respond speedily, they tend to do so on the basis of a superficial understanding of what cybercrime truly is. There is a tendency to take any crime which has an element of the internet or of a computer system to it and uncritically label it as a cybercrime.

The study revealed that the hypothesis was partially inaccurate. While it is true that cybercrime is proliferating at an exponential rate, with which governments struggle to keep pace, the Cybercrimes Act may be accepted as progressive. It appears to have been drafted with a demonstrable understanding of what cybercrime is and how to respond to it appropriately. However, it must be accepted also that the Cybercrimes Act is not a perfect piece of legislation. Hence, this study would have recommended certain amendments that ought to have been made to the Cybercrimes Act before it was enacted into law.

7.2 Philosophical Resources

The main research question posed by this study was whether one could describe parameters for establishing whether certain crimes involving computers and cyberspace are cybercrimes proper. To that end, the study proposed the adoption of a two-part framework. The first part of the framework comprises the Gordon and Ford Categorisation (G&FC), while the second part requires the application of the Routine Activities Theory (RAT).

Gordon & Ford devised a way of determining whether an offence was a Type I cybercrime or a Type II cybercrime by way of two questions. The first question asks whether the offence is committed with the use of crimeware. The second question asks whether, from the perspective of the suitable target, the attack is a once-off occurrence. If the answer to both questions is yes, then the offence is a Type I cybercrime; but if the answer to both questions is no, then the offence is a Type II cybercrime.

RAT is a theory which has undergone many developments over the years and it has been found to be effective in dealing with almost all questions regarding criminal conduct. The main question which RAT tries to answer relates to the social factors or structures that have to be in place to allow for the successful commission of a crime. This approach contrasts with other theories of crime which are focused on the criminal herself and on the social or biological factors that motivate or drive her to offend. The fact that the offender is inclined to offend is taken as a given and so the social structures that exist to allow for the

commission of the crime are what are of interest. Given that RAT was developed in the 1970s, it was concerned only with traditional terrestrial crimes. However, as was seen in this study, the core principles of RAT may be applied with some success to cybercrimes.

The aetiological formula of RAT is worth restating here: in order for the commission of a crime to occur, the motivated offender and the suitable target must converge in space and time and such convergence must be accompanied by the absence of a capable guardian. This is as true of cybercrimes as it is of terrestrial crimes.

7.3 The Structure of the Study

Chapter One of this study introduced the issues to be canvassed, by outlining the landscape of cybercrime. Chapter Two continued this by unpacking cybercrime, whilst laying the foundation for what would constitute the philosophical map of the study in the form of RAT and the G&FC. This philosophical foundation framed the structure that the rest of the study would take.

Three of the subsequent chapters focused upon the constitutive elements of RAT. In this regard, Chapters Three, Four and Six contains the substantive discussion of the Cybercrimes Act. Chapter Three was written against the backdrop of the motivated offender, Chapter Four was constructed in relation to the suitable target and the ambit of capable guardian informed the composition of Chapter Six.

Furthermore, Chapter Three and Chapter Four discussed the specific offences contained in the Cybercrimes Act, with Type I crimes being examined in Chapter Three and Type II crimes in Chapter Four. Chapter Five reviewed the procedural provisions found in the Act and the Budapest Convention, with particular attention being paid to jurisdictional issues and international co-operation. Chapter Six brought things together by proposing a method of tackling cybercrime, in the form of the Designated Point of Contact (DPoC) as the cyber capable guardian.

7.4 Offences in the Cybercrimes Act

It will be recalled that the G&FC proposes that cybercrimes be categorised into Type I and Type II, and whether an offence is Type I or Type II depends on the characteristics that it displays. This categorisation was founded in the assertion that cybercrimes exist on a spectrum, which has Type I cybercrimes at one end and Type II cybercrimes at the other.

The original version [B—2015] of the Cybercrimes Act has all the offences listed together in a single chapter. It makes no distinctions between different types of cybercrimes, meaning that all were treated as if they were the same. After deliberations with interested parties and public participation, the drafters of version [B6—2017] of the Cybercrimes Bill created two categories of offences, apparently following the G&FC. The latest version of the Cybercrimes Bill — [B 6B—2017] — provides for offences in Part I and II of Chapter 2. An examination of the offences included in version [B 6B—2017] revealed that all but one of the crimes in Part I of Chapter 2 could be categorised as Type I cybercrimes. The crime of cyberfraud is the outlier as it does not meet the minimum requirements to be considered a Type I cybercrime.

The main purpose of a piece of crime legislation is to designate certain types of behaviours as criminal offences and to provide for measures that must be taken to punish those behaviours. Therefore, it is necessary for such legislation to be drafted with a clear and concise remit. Cybercrime poses a special kind of challenge because it exists on a spectrum, which implies that the offences covered by the Cybercrimes Act need to be carefully selected in order to avoid a "shotgun" approach, where every single unsavoury act which occurs on the internet is called a cybercrime. Unfortunately, the Cybercrimes Act has not been immune to this kind of temptation.

It was determined in this study that, while there are Type I cybercrimes and Type II cybercrimes, there are also crimes which do not fall into either category. It is debatable whether they fall within the spectrum or completely without it. Whatever the case may be, the recommendation is to exclude such crimes from the Cybercrimes Act altogether. The crimes in question are the crimes of cyberfraud and data messages which incite violence (online incitement), contained in section 8 and section 14, respectively, of the Cybercrimes Act.

The study also introduced the concept of a *true cybercrime* and postulated that these are the only crimes that ought to be accommodated in the Cybercrimes Act. It argued that, in order determine which crimes may be considered true cybercrimes, it is necessary to incorporate certain minimum requirements that will act as a threshold for inclusion in the Cybercrimes Act. True cybercrimes meet two minimum requirements: firstly, the offence needs to be an attack upon the confidentiality, integrity and/or availability of a computer

system, the so called CIA triad; and, secondly, the offence must be computer dependent as opposed to being computer enabled. Only if both of these minimum requirements have been met, in addition to the criteria describing Type I cybercrimes, may offences be determined to be true cybercrimes. This means that while Type II cybercrimes are considered to be cybercrimes, they are not true cybercrimes in the strict sense. Therefore, for purposes of the Cybercrimes Act, they ought to be excluded.

Type I cybercrimes are easy to identify using the G&FC and the minimum requirements. They include offences such as hacking, distributed denial of service (DDoS) attacks, phishing, and cyber extortion through ransomware. Type II cybercrimes, by contrast, may be relatively more challenging to determine because their categorisation depends on the absence, rather than the presence, of certain characteristics. For instance, a Type II cybercrime may be committed using anything that is not considered to be crimeware. Also, the offence must be a repeated attack rather than a once-off event from the perspective of the suitable target. Any iteration suffices. Furthermore, with regard to the minimum requirements, Type II cybercrimes are computer enabled, which tends to result in the suitable target typically being a human being rather than a computer system. Therefore, there is no attack on the CIA triad. All of this results in Type II cybercrimes having a considerably broader scope than Type I cybercrimes.

The consequence of the overly broad scope of the Type II cybercrimes is that many offences are mischaracterised as cybercrimes, simply because there was some kind of computer presence when the crime was committed, regardless of how insignificant that presence. Cyberfraud and data messages which incite damage to property or violence were mentioned as examples of such offences.

In the Cybercrimes Act, cyberfraud is placed in the same category as the crimes referred to in this study as Type I cybercrimes. This placing is incorrect because some of the means by which cyberfraud is perpetrated, such as advance fee fraud crimes, do not meet the minimum requirements of being an attack upon the CIA triad and being computer dependent. They also are committed without the use of crimeware. Additionally, the attack tends to be a repeated or prolonged attack from the perspective of the suitable target.

If these offences cannot be categorised as Type I cybercrimes, the question becomes whether they can be classified as Type II cybercrimes instead? This study has argued that, while Type II cybercrimes are recognisable cybercrimes, the offences of cyberfraud and data messages which incite damage to property or violence do not fit under the banner of Type II cybercrimes either. Type II cybercrimes are categorised as cybercrimes because the role which cyberspace and computer systems play in their commission is significant enough to elevate them from ordinary crimes to cybercrimes. The role of the internet in cyberfraud and data messages which incite damage to property or violence is not significant enough to move these offences onto the cybercrime spectrum. Therefore, the study recommends that these two crimes be excluded from the Cybercrimes Act altogether.

It was argued further that cyberfraud and data messages which incite damage to property or violence are not the only offences that ought to be excluded from the Cybercrimes Act. In fact, it is recommended that all offences categorised as Type II cybercrimes ought to be excluded. The crux of this argument is that all the Type II cybercrimes incorporated in the "malicious communication" chapter of the Cybercrimes Act have existing laws that address their terrestrial or offline manifestations. For example, the crime of online harassment and non-consensual pornography are covered by the Protection from Harassment Act and the Sexual Offences Act respectively. It would be preferable if the existing legislation were developed to cater for the role that the internet plays in enabling these offences rather than to attempt to deal with them in Cybercrimes Act.

Given the challenges of cybercrime, it is necessary for the law governing it to be as precise as possible and to be guided by a singular and focused mandate of addressing only true cybercrimes. The inclusion of offences which already are catered for elsewhere is redundant and counterproductive, and is particularly problematic when it comes to issues relating to the enforcement of the laws.

7.5 International Co-operation and Law Enforcement

By way of introduction to the third constitutive element of RAT, it was considered necessary to engage with the procedural aspects of the Cybercrimes Act, namely, jurisdiction, international co-operation and mutual assistance. The procedural provisions in the Act are in keeping with the Budapest Convention, except that they are concerned more with the

domestic perspective than the international one. Nevertheless, they do not run contrary to international norms and standards.

On the question of jurisdiction, the Act engages with accepted principles in both the domestic and international sense. Unfortunately, it is silent on the question of extradition for the most part. It is unclear whether this is an inadvertent omission on the part of the drafters or whether one should assume that the question is encompassed within the ambit of the Extradition Act.

The Cybercrimes Act also accords with the Budapest Convention when it comes to preservation of data, disclosure of preserved data and so forth. It is here that the Act provides for more direction on the relationship between law enforcement, service providers and other interested parties. It sets out clearly the obligations of each party, as well as the sanctions for non-compliance. It further details the procedures that must be followed to obtain certain information, and stipulates the chain of command.

The issue of enforcement was discussed in this study insofar as it relates to the third constitutive element of RAT, which is the capable guardian. It sought to answer the question of how to prevent the commission of a cybercrime.

The capable guardian is someone (or something) who has the ability to prevent the commission of a crime by intersecting in space and time with the motivated offender and the suitable target. The idea of the capable guardian, like the other elements of RAT, has undergone numerous developments over the years. Unfortunately, none of the developments appreciate the challenges of cybercrime. Nevertheless the idea of a capable guardian itself remains applicable to combating cybercrime, if it is expanded appropriately.

The Cybercrimes Act provides for the creation of an office called the Designated Point of Contact (DPoC) which is to be housed within the South African Police Services (SAPS). The office must ensure collaboration with the South African National Prosecution Authority (NPA) also. In this study, the DPoC is identified as being an appropriate capable guardian in the fight against cybercrime. However, it is argued that the DPoC must incorporate artificial intelligence (AI) and machine learning technology to create an entity which the study has named the *cyber capable guardian*. Whilst the DPoC would act as the overall capable guardian with broad oversight powers, it is the cyber capable guardian

which would engage in the actual investigation of cybercrimes and the gathering of information. It is necessary for there to be a cyber capable guardian which is premised on machine learning technology because true cybercrimes rely crucially upon crimeware, meaning that in many cases they also rely on machine learning technology. It would make sense, therefore, that that which seeks to combat cybercrime should have the same capabilities as the cybercriminals themselves.

When a cybercrime is committed, the motivated offender behind the attack is an actual human being but, because of the nature of cybercrime, she need execute only computer commands which instruct a computer system and crimeware to commit the actual offence, such as a DDoS attack. This means that it is possible for a single motivated offender to attack a thousand suitable targets with just a few keystrokes. Given that the capable guardian can be effective in preventing a crime only by coming together in time and space with the motivated offender and the suitable target, it is necessary that the cyber capable guardian be a “something”, rather than a “someone”, with the capacity to be in a thousand places at the same time.

The cyber capable guardian has to be based upon machine learning technology so that it can teach itself new commands and actions by learning from the information that it gathers. This means that the engineers employed by the DPoC would need only to provide the cyber capable guardian with initial data sets, which would allow it to learn from patterns that it observes in a smart and intuitive way. Ultimately, it would be able to adapt to all the new methods that motivated offenders use to commit cybercrimes, provided that it is maintained and kept up to date by the DPoC.

The study recommends that one of the ways of ensuring that the cyber capable guardian benefits from consistent investments in research and design is to create the DPoC as an independent and privately incorporated agency, outside the province of the SAPS. This is important because it would give the DPoC agency sufficient financial freedom and a wide enough margin of autonomy to allow it to be forward-thinking and innovative in its confrontation with cybercrime.

All in all, this study has shown that cybercrime is a complex challenge which demands unconventional solutions. The Routine Activities Theory is a good foundation upon which to build effective responses to cybercrime. It is even more effective if it is reinforced

with the G&FC and the minimum requirements. The Cybercrimes Act is drafted well and, contrary to the initial hypothesis, it does appear to be informed by a good understanding of what cybercrime is. The only serious shortfall from which the Cybercrimes Act suffers relates to Type II cybercrimes, which ought to have no place amongst its provisions at all because they already are dealt with adequately in existing laws. Finally, in order for any of the measures against cybercrime to succeed, the DPoC must be created as an independent agency which will invest in the creation of a machine learning cyber capable guardian.

BIBLIOGRAPHY

PRIMARY SOURCES

International Instruments, Legislation and Case Law

Communications Decency Act 47 USC §230(c)(1) (2012), also known as Title V of the Telecommunications Act of 1996.

Council of Europe Convention on Cybercrime, Budapest 23.XI (2001).

Indictment for United States v Moore No CR13-00917 C.D. Cal. (2013), available at https://www.wired.com/images_blogs/threatlevel/2014/01/revenge-porn-Moore-Evens-indictment.pdf (visited 22 July 2017).

Lester v Mineta, Second Amended Complaint No C-04-3074 SI (ND Cal 2006), 2006 WL 104226.

Organisation of American States (undated) "The G8 24/7 Network of Contact Points Protocol Statement", available at http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf (visited 2 January 2020).

Domestic Legislation and Case Law

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007.

Customs and Excise Act 91 of 1964.

Customs Control Act 31 of 2014.

Electronic Communication and Transactions Act 25 of 2002.

Electronic Communications Act 36 of 2005.

Ex parte Lebowa Development Corporation Ltd 1989 (3) SA 71 (T) 101.

Extradition Act 67 of 1962.

Films and Publications Act 65 of 1996.

Financial Intelligence Centre Act 38 of 2001.

Gardner 2011 (1) SACR 570 (SCA).

Interception and Monitoring Prohibition Act 127 of 1992.

International Co-operation in Criminal Matters Act 75 of 1996.

Myeza 1985 (4) SA 30 (T).

National Strategic Intelligence Act 39 of 1994.

Nkosiyana 1966 (4) SA (A).

Prevention of Organised Crime Act 121 of 1998.

Protection from Harassment Act 17 of 2011.

Regulation of Interception and Provision of Communication-Related Information Act 70 of 2002.

Riotous Assemblies Act 17 of 1956.

Segale 1960 (1) SA 721 (A).

State Information Technology Agency Act 88 of 1998, as amended by SITA Amendment Act 38 of 2002.

Superior Courts Act 10 of 2013.

Tax Administration Act 28 of 2011.

SECONDARY SOURCES

Books

Burchell J (2016) *Principles of Criminal Law* (5ed) Claremont: Juta & Co Ltd.

Castells M (2002) *The Internet Galaxy: Reflections on the Internet, Business and Society* New York: Oxford University Press.

Clegg B (2017) *Big Data: How the Information Revolution is Transforming our Lives* London: Icon Books Ltd.

Clough B & Mungo P (1992) *Approaching Zero: Data Crime and the Computer Underworld* London: Faber and Faber.

Clough J (2015) *Principles of Cybercrime* (2ed) Cambridge: Cambridge University Press.

Dodge M & Kitchin R (2001) *Atlas of Cyberspace: Volume 158* London: Addison-Wesley.

Felson M & Boba RL (eds) (2010) *Crime and Everyday Life* (4ed) London: Sage Publications.

Finch E (2007) “The Problem of Stolen Identity and the Internet” in Jewkes Y (ed) *Crime Online* London: Willan Publishing.

Furnell S (2002) *Cybercrime: Vandalising the Information Society* London: Addison Wesley.

Glaser D (1971) *Social Deviance* Ann Arbor: Markham Publishing Company.

Grabosky P & Smith R (2001) “Telecommunication Fraud in the Digital Age: The Convergence of Technologies” in Wall D (ed) *Crime and the Internet* London: Routledge.

Hirschi (1969) *Causes of Deliquency* Berkley: University of California Press.

Johnson (1985) *Computer Ethics* Englewood Cliffs, New Jersey: Prentice Hall. (2nd edn, 1994; 3rd edn, 2001.)

Krebs B (2014) *Spam Nation: The Inside Story of Organized Cybercrime – From Global Epidemic to Your Front Door* Naperville: Source Books Inc.

Milton JRL (1996) *South African Criminal Law and Procedure: Volume 2* (3ed) Cape Town: Juta.

Mitchell TM (2006) *The Discipline of Machine Learning* Pittsburgh: Carnegie Mellon University.

Muncie J (1999) *Youth and Crime: A Critical Introduction* London: Sage.

Newman G & Clarke R (2003) *Superhighway Robbery: Preventing Ecommerce Crime* Cullompton: Willan Press.

Olson P (2013) *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* London: William Heinemann.

Russel S & Norvig P (2016) *Artificial Intelligence: A Modern Approach* (3ed) Essex: Pearson.

Schell BH, Dodge JL & Moutsatsos SS (2002) *The Hacking of America: Who’s Doing It, Why, and How* Westport: Quorum Books.

Schneier B (2018) *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* New York City: W. W. Norton & Company.

Snyman CR (1992) Criminal Law (3ed) Durban: Butterworths.

Tavani (2007) *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology* (2 ed) Hoboken, New Jersey: John Wiley & Sons.

Taylor P (1999) *Hackers: Crime in the Digital Sublime* London: Routledge.

Chapters in Books

Beavon Brantingham & Brantingham (1994) “The Influence of Street Networks on the Patterning of Property Offenses” in Clarke RV (ed) *Crime Prevention Studies: Volume II* New York: Willow Tree Press.

Bougaardt & Kyobe (2011) “Investigating the Factors Inhibiting SMEs from Recognising and Measuring Losses from Cybercrime in South Africa” in Grant K (ed) *ICIME Proceedings of the 2nd International Conference on Information Management and Evaluation* Toronto: Ryerson University.

Brickwell (2017) “Theorising power online” in Martellozzo & Jane (eds) *Cybercrime and its victims* New York: Routledge.

Broeders & van den Berg (2020) “Governing Cyberspace: Behaviour, Power and Diplomacy” in Broeders & van den Berg (eds) *Governing Cyberspace* London: Rowman & Littlefield.

Felson (2014) “Linking criminal choices, routine activities, informal control, and criminal outcomes” in Clark *The Reasoning Criminal: Rational choice perspectives on offending* New York: Routledge

Hickle (2017) “Victims of sex trafficking” in Martellozzo & Jane (eds) *Cybercrime and its victims* New York: Routledge.

Jane (2017) “Gendered cyberhate and victim blaming” in Martellozzo & Jane (eds) *Cybercrime and its victims* New York: Routledge.

Johnson (2000) ‘Should Computer Programs be Owned?’ in Baird, Ramsower & Rosenbaum, (eds.), *Cyberethics – Social and Moral Issues in the Computer Age* New York: Prometheus Books.

Martellozzo & Jane (2017) ‘victims of cybercrime in the small “i” internet’ in Martellozzo & Jane (eds) *Cybercrime and its victims* New York: Routledge.

Martellozzo (2017) ‘Online sexual grooming’ in Martellozzo & Jane (eds) *Cybercrime and its victims* New York: Routledge.

Ryngaert (2016) "Territory in the law of jurisdiction: imagining alternatives." In Netherlands Yearbook of International Law The Hague: TMC Asser Press.

Sofaer AD & Goodman SE (2001) “Cyber Crime and Security — The Transnational Dimension” in Sofaer AD & Goodman SE (eds) *The Transnational Dimension of Cyber Crime and Terrorism* Stanford: Hoover Institution Press.

Tavani (2010) “The Foundationalist debate in computer ethics” in Floridi (ed) *The Cambridge Handbook of Information and Computer Ethics* Cambridge: Cambridge University Press.

Journal Articles and Conference papers

Adams P (1998) “Network Topologies and Virtual Place” 88 *Annals of the Association of American Geographers* 88–106.

Antonakakis, April, Bailey, Bernhard, Bursztein, Cochran, J & Zhou (2017) “Understanding the mirai botnet” in *26th {USENIX} security symposium ({USENIX} Security 17)* 1093-1110.

Asongu and Biekpe (2017) Government Quality Determinants of ICT Adoption in Sub-Saharan Africa MPRA Paper No. 81704

August R (2002) “International Cyber-Jurisdiction: A Comparative Analysis” 39 *American Business Law Journal* 531-573.

Azad, Mazid, & Sharmin (2017) “Cybercrime problem areas, legal areas and the cybercrime law” 3(5) *International Journal of New Technology and Research* 1-6.

Bansla, Swati & Gupta (2019) *"Social engineering: A technique for managing human behaviour”* 5(1) Journal of Information Technology and Sciences 18-22.

Bennett R (1991) “Routine Activities: A Cross-National Assessment of a Criminological Perspective” 70(1) *Social Forces* 147– 163.

Brenner S & Koops BJ (2004) “Approaches to Cybercrime Jurisdiction” 4(1) *Journal of High Technology Law* 1-46.

Brody G, Mulig E & Kimball V (2007) “Phishing, Pharming and Identity Theft*”* 11(3) *Academy of Accounting and Financial Studies Journal* 43-56.

Burton P & Mutongwizo T (2009) “Inescapable Violence: Cyber Bullying and Electronic Violence against Young People in South Africa” 8 *Centre for Justice and Crime Prevention* 1-12.

Calo, Evtimov, Fernandes, Kohno, & O'Hair, (2018) “Is Tricking a Robot Hacking?” *University of Washington School of Law Research Paper* 1 – 20.

Calvert C (2015) “Revenge Porn and Freedom of Expression: Legislative Pushback to an Online Weapon of Emotional and Reputational Destruction*”* 2A(1) *Fordham Intellectual Property, Media & Entertainment Law Journal* 673 – 702.

Cassim F (2010) “Addressing the Challenge Posed by Cybercrime: A South African Perspective” 5(3) *Journal of International Commercial Law and Technology*-118-123.

Chigada & Kyobe (2018) “Evaluating Factors Contributing to Misalignment of the South African National Cybeersecurity Policy Framework” In *International Conference on Information Resources Management (CONF-IRM)*. Association for Information Systems.

Cicchetti D & Toth S (1995) “A Developmental Psychopathology Perspective on Child Abuse and Neglect” 34(5) *Journal of the American Academy of Child & Adolescent Psychiatry* 541-565.

Citron D & Franks M (2014) “Criminalising Revenge Porn” 49 *Wake Forest Law Review* 345 – 391.

Cohen L & Felson M (1979) “Social Change and Crime Rate Trends: A Routine Activity Approach” 44(4) *American Sociological Review* 588 – 608.

Cohen L & Felson M (1980) “Human Ecology and Crime: A Routine Activity Approach” 8(4) *Human Ecology* 389 – 406.Felson M (1995) “Those who Discourage Crime” 4 *Crime and Place* 53-66.

Costello & Laub (2020) “Social control theory: The legacy of Travis Hirschi's causes of delinquency” *3 Annual Review of Criminology* 21-41.

Cross C, Smith RG & Richards K (2014) “Challenges of Responding to Online Fraud Victimisation in Australia” 474 *Trends & Issues in Crime and Criminal Justice*.

Dodge (2020) “Jurisdiction, State Immunity, and Judgments in the Restatement (Fourth) of U.S. Foreign Relations Law” 19 *Chinese Journal of International Law*, UC Davis Legal Studies Research Paper Forthcoming available at SSRN: https://ssrn.com/abstract=3547660 or http://dx.doi.org/10.2139/ssrn.3547660 (visited 15 October 2021).

El-Mawass, Honeine & Vercouter (2018) “Supervised classification of social spammers using a similarity-based Markov Random Field approach” MISNC, Saint-Etienne, France 1-9.

Galli (2018) “How ethics impacts hacktivism: a reflection of events” *3*(1) *International Journal of Qualitative Research in Services* 11-20.

Ghimire & Selvaraj (2018) “A survey on bitcoin cryptocurrency and its mining” in *2018 26th International Conference on Systems Engineering (ICSEng)* 1-6 IEEE.

Goodman & Brenner (2002) “The Emerging Consensus on Criminal Conduct in Cyberspace.” 10(2) *International Journal of Law and Information Technology* 139-223.

Gordon S & Ford R (2006) "On the Definition and Classification of Cybercrime." 2(1) *Journal in Computer Virology* 13-20.

Gunkel DJ (2005) "Editorial: Introduction to Hacking and Hacktivism" 7(5) *New Media & Society* 595-597.

Gyunka & Abikoye (2017) "Analysis of human factors in cyber security: A case study of anonymous attack on HBGary" 21(2) *Computing and Information System Journal* 1 – 41.

Hajizadeh, Phan & Bauschert (2018) "Probability analysis of successful cyber attacks in sdn-based networks" IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) IEEE 1-6.

Herselman M & Warren M (2004) "Cyber Crime Influencing Businesses in South Africa" *Issues in Informing Science & Information Technology*254-266.

Himma (2003) "The Relationship between the Uniqueness of Computer Ethics and Its Independence as a Discipline in Applied Ethics" Ethics and Information Technology 5(4), 225–237

Hollis-Peel ME, Reynald DM, Van Bavel M, Elffers H & Welsh BC (2011) "Guardianship for Crime Prevention: A Critical Review of the Literature" 56 *Crime, Law and Social Change* 53–70.

Holt, Leukfeldt, & van de Weijer (2020) "An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites" *47*(4) *Criminal Justice and Behavior* 487-505.

Johannes König, Daniela J. Jäger-Biela & Nina Glutsch (2020) "Adapting to online teaching during COVID-19 school closure: teacher education and teacher competence effects among early career teachers in Germany"43(4) European Journal of Teacher Education, 608 - 622.

Johnson & Miller (2008) *"Un-making Artificial Moral Agents"*, Ethics and Information Technology 10, 123–133.

Johnson (1997) "Is the Global Information Infrastructure a Democratic Technology?" Computers and Society 27, 20–26.

Johnson (2006) "Computer Systems: Moral Entities but Not Moral Agents" 8(4) Ethics and Information Technology 195–204.

Johnson, Davies, Murray, Ditta, Belur & Bowers (2017) "Evaluation of operation swordfish: a near-repeat target-hardening strategy" *13*(4) *Journal of experimental criminology* 505-525.

Kigerl (2021) “Routine activity theory and malware, fraud, and spam at the national level” *Crime, Law and Social Change* 1-22.

Kritzinger E & Von Solms SH (2010) “Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement” 29(8) *Computers & Security* 840-847.

Kshetri (2019) “Cybercrime and Cybersecurity in Africa” 22(2) Journal of Global Information Technology Management 77-81.

Kutz R (1986) “Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act” 27 *William and Mary Law Review* ‘783 – 831.

Lepofsky R (2006) “Cyberextortion by Denial-of-Service Attack” 53(6) *Risk Management Magazine*.

Leukfeldt & Yar. (2016) “Applying routine activity theory to cybercrime: A theoretical and empirical analysis” *37*(3) *Deviant Behavior* 263-280.

Leukfeldt RE & Yar M (2016) “Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis” 37(3) *Deviant Behaviour* 263-280.

Li, Shin & Wong (2021) “Crytocurrency Pump & Dump” *Available at SSRN 3267041*, 1 – 60.

Mabunda S (2017) “Applying the Gordon & Ford Categorisation and the Routine Activities Theory to Cybercrime: A Suitable Target” in Cunningham P & Cunningham M (eds) *IST Africa Conference Proceedings* 1-10.

Maimon & Louderback (2019) “Cyber-dependent crimes: an interdisciplinary review” 2 Annual review of Criminology 191 -216.

Messit M (2014) “Cyberbullying Happens in Code. Break It” 79(9) *The Education Digest Ann Arbor* 51 – 54.

Mirkovic J & Reiher P (2004) “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms”

34(2) *ACM SIGCOMM Computer Communications Review* 39 – 53.

Miró F (2014) “Routine Activity Theory” *The Encyclopedia of Theoretical Criminology* 1-7.

Mondal, Das, Nath, & Goswami (2020) “Review Study on Different Attack Strategies of Worm in a Network” *17*(2) *Webology* 363-375.

Moore (2018) “Anonymity, pseudonymity, and deliberation: Why not everything should be connected” *26*(2) *Journal of Political Philosophy* 169-192.

Narcyz Roztocki, Piotr Soja & Heinz Roland Weistroffer (2019) “The role of information and communication technologies in socioeconomic development: towards a multi-dimensional framework” Information Technology for Development 25(2), 171-183.

Neuhaus (2020) "A (Nudge) Psychology Reading of the ‘Nigerian Scam’" 3(3) Brolly 7-28.

Olowu D (2009) “Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa” 1 *Journal of information, Law & Technology* 1-18.

Oussous, Benjelloun, Lahcen, & Belfkih (2018) “Big Data technologies: A survey” *30*(4) *Journal of King Saud University-Computer and Information Sciences* 431-448.

Parker DB (2010) “Our Excessively Simplistic Information Security Model and How to Fix it” 8(7) *ISSA Journal* 12-21.

Pedro D (2012) "A Few Useful Things to Know about Machine Learning" 55(10) *Communications of the ACM* 78-87.

Pokwana & Kyobe (2016) “Investigating the Misalignment in the Existing ELegislation of South Africa” In *International Conference on Information Resources Management (CONF-IRM)* Association for Information Systems AIS Electronic Library (AISeL).

Poole E (2015) “Fighting back against Non-Consensual Pornography” 49 *University of San Francisco Law Review* 181 – 214.

Reyns (2017) “Routine activity theory and cybercrime: A theoretical appraisal and literature review” *Technocrime and criminological theory* 35-54.

Reyns BW, Henson B & Fisher BS (2016) “Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept from Routine Activity Theory as it Applies to Online Forms of Victimization” 32(2) *Journal of Contemporary Criminal Justice* 148–168.

Rich (2017) “You can trust me: a multimethod analysis of the Nigerian email scam” 31(1) Security Journal 208 -225.

Richterich, & Wenz (2017) “Introduction: Making and hacking” *3*(1) *Digital Culture & Society* 5-22.

Romagna (2020) “Hacktivism: Conceptualization, Techniques, and Historical View” *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 743-769.

Sallavaci (2017) “Combating cyber dependent crimes: The legal framework in the UK” in *International Conference on Global Security, Safety, and Sustainability* 53-66.

Shahrear, Chakraborty, Islam, & Habiba (2018) “Analysis of Computer Virus Propagation Based on Compartmental Model” *7*(1-2) *Applied and Computational Mathematics* 12-21.

Sieber U (1998) “Legal Aspects of Computer-Related Crime in the Information Society”

Comcrime Study prepared for the European Commission.

Smith RG, Holmes MN & Kaufman P (1996) “Nigerian Advance Fee Fraud” 121 *Trends and Issues in Criminal Justice* 4 – 5.

Snail S (2009) “Cybercrime in South Africa – Hacking, Cracking and Other Unlawful Online Activities” 138 *Journal of Information, Law & Technology* 1-13.

Stander A, Dunnet A & Rizzo J (2009) “A Survey of Computer Crime in South Africa” *Proceedings of ISSA 2009 Conference* 217-226.

TataRoa & Reddy (2019) “The Cybercrime underground economy approach” 7(6) IJCST.

Tavani (2002) “The Uniqueness Debate in Computer Ethics: What Exactly Is at Issue, and Why Does it Matter?” 4(1) Ethics and Information Technology

Tavani H (2000) “Defining the Boundaries of Computer Crime: Privacy, Break-Ins and Sabotage in Cyberspace” *ACM SIGCAS Computers and Society* 3-9.

Thomas D (2002) “Notes from the Underground: Hackers as Watchdogs of Industry” *Online Journalism Review.*

Viliç (2019) “Phishing and pharming as forms of identity theft and identity abuse” *13*(13) *Balkan Social Science Review* 43-57.

Wadhwa & Neerja (201) "A Review on Cyber Crime: Major Threats and Solutions" 8(5) International Journal of Advanced Research in Computer Science.

Wang AH (2010) "Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach" *IFIP Annual Conference on Data and Applications Security and Privacy* 335-342.

Whitty (2018) “419 – It’s just a game: pathways to cyber-fraud criminality emanating from West Africa.” International Jouranl of Cyber Criminology 12(1) 97 -114.

Williams ML (2015) “Guardians upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level” 56(1) *British Journal of Criminology* 21-48.

Xu Z, Hu Q & Zhang C (2013) “Why Computer Talents Become Computer Hackers” 56(4) *Communications of the ACM* 64 – 74.

Yar M (2005a) “The Novelty of Cybercrime: An Assessment in Light of Routine Activities Theory” 2 *European Journal of Criminology* 407-427.

Yar M (2005b) “Computer Hacking: Just Another Case of Juvenile Delinquency?” 44(4) *The Howard Journal of Criminal Justice* 387–399.

Zając (2021) "The European Arrest Warrant in Designer Drugs Cases. With or Without Verification of Double Criminality?" European Journal on Criminal Policy and Research 1-15.

Zhang (2018) “Application of Artificial Intelligence Technology in Computer Network Security” *20*(6) *International Journal of Network Security* 1016-1021.

Zou & Schaub (2018) *"Concern But No Action: Consumers' Reactions to the Equifax Data Breach."* Extended abstracts of the 2018 CHI conference on human factors in computing systems, 1 – 6.

News Reports and other and Online Sources

Abrams (2019) “Power Company has security breach due to downloaded game” Bleeping Computer available at https://www.bleepingcomputer.com/news/security/power-company-has-security-breach-due-to-downloaded-game/ (visited 3 October 2021).

Addley & Halliday J (2010) “Operation Payback Cripples MasterCard Site in Revenge for WikiLeaks Ban” *The Guardian*, available at https://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks (visited 4 April 2019).

Anonymous Official (2014) “Anonymous Documentary: How Anonymous Hackers Changed the World” *YouTube*, available at https://www.youtube.com/watch?v=FAECyLvSCHg (visited 4 April 2019).

Antihack.me (2018) “The Shades of Hacking: Black, White & Grey” *Medium,* available at https://medium.com/@Antihack.me/the-shades-of-hacking-black-white-grey-c15709dcec8a (visited 4 April 2019).

Barkham (2008) “Hackers Declare War on Scientologists amid Claims of Heavy-Handed Cruise Control” *The Guardian*, available at https://www.theguardian.com/technology/2008/feb/04/news (visited 4 April 2019).

BBC News (2017) “NHS Cyber-Attack: GPs and Hospitals Hit by Ransomware”, available at http://www.bbc.com/news/health-39899646 (visited 4 April 2019).

BBC News Africa (2004) “Huge Nigeria Scam Trial Collapses”, available at http://news.bbc.co.uk/2/hi/africa/3909233.stm (visited 4 April 2019).

Berrada (2020) “Cybercrime: West African banks are underprotected” The Africa Report available at https://www.theafricareport.com/22644/cybercrime-west-african-banks-are-under-protected/ (visited 30 September 2021)

CBS News (2017) "Global Cyberattack Strikes Dozens of Countries, Cripples UK Hospitals" available http://www.cbsnews.com/news/hospitals-across-britain-hit-by-ransomware-cyberattack/ (visited 4 April 2019).

Cimpanu (2019) “Ransomware incident leaves some Johannesburg residents without electricity” ZDNet available at https://www.zdnet.com/article/ransomware-incident-leaves-some-johannesburg-residents-without-electricity/ (visited 2 October 2021)

Cimpanu (2019b) “’Carpet-bombing’ DDoS attack takes down South African ISP for an entire day” ZDNet available at https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/ (visited 3 October 2021).

Cimpanu (2019c) “City of Johannesburg held for ransom by hacker gang” ZDNet available at zdnet.com/article/city-of-johannesburg-held-for-ransom-by-hacker-gang/ (visited 3 October 2021).

Clement (2020) “Internet usage worldwide – Statistics and facts” available at https://www.statista.com/topics/1145/internet-usage-worldwide/ (visited 1 October 2020).

Cowen K (2015) “Anonymous Africa – The Hackers that are Taking on South Africa” *Zululand Observer*, available at https://zululandobserver.co.za/117693/anonymous-africa-the-hackers-who-are-taking-on-south-africa/ (visited 4 April 2019).

Cuozzo S (2015) “The Genius behind ‘Headless Body Found in Topless Bar’ Headline Dies at Age 74” *New York Post*, available at https://nypost.com/2015/06/09/new-york-post-editor-and-film-critic-vincent-musetto-dies-at-74/ (visited 4 April 2019).

Department of Justice and Constitutional Development (2021) Media Statement “Justice and Constitutional Development updates on recent ransomware attack” Available at https://www.gov.za/speeches/justice-and-constitutional-development-updates-recent-ransomware-attack-20-sep-2021-0000 (visited 30 September 2021).

Digital Attack Map (2013) “What is a DDoS Attack” available at https://www.digitalattackmap.com/understanding-ddos/ (visited 4 April 2019).

Electronic Frontier Foundation (no date) “CDA 230, the Most Important Law Protecting Internet Speech” available at https://www.eff.org/issues/cda230 (visited 4 April 2019).

FBI (2012) "'Ransomware' Locks Computer, Demand's Payment" *US Department of Justice*, available at https://www.fbi.gov/news/stories/new-internet-scam (visited 4 April 2019).

FBI Press Release (2013) "Nine Individuals Indicted in One of the Largest International Penny Stock Frauds and Advance Fee Schemes in History" *US Department of Justice*, available at https://archives.fbi.gov/archives/newyork/press-releases/2013/nine-individuals-indicted-in-one-of-the-largest-international-penny-stock-frauds-and-advance-fee-schemes-in-history (visited 4 April 2019).

FBI Report (2012) "Internet Social Networking Risks" *US Department of Justice*, available at https://www.fbi.gov/file-repository/internet-social-networking-risks-1.pdf/view (visited 15 June 2017).

Fenton S (2016) "The Myths around Revenge Porn" *IOL*, available at www.iol.co.za/entertainment/celebrity-news/the-myths-about-revenge-porn-2020793 (visited 4 April 2019).

Filipovic (2013) "'Revenge Porn' is about Degrading Women Sexually and Professionally" *The Guardian*, available at http://www.theguardian.com/commentisfree/2013/jan/28/revenge-porn-degrades-women (visited 4 April 2019).

Finlay & Payne (2019) "Why international law is failing to keep pace with technology in preventing cyber attacks" The Conversation available at https://theconversation.com/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks-111998 (visited on 11 October 2021).

Gardner B (2015) "You'll be Outraged by How Easy it was to Get You to Click on this Headline" *Wired*, available at https://www.wired.com/2015/12/psychology-of-clickbait/ (visited 4 April 2019).

Gatlan (2019) "Garmin SA Shopping portal breach leads to theft of payment data" Bleeping Computer https://www.bleepingcomputer.com/news/security/garmin-sa-shopping-portal-breach-leads-to-theft-of-payment-data/ (visited 3 October 2021).

Goodin D (2014). "Feds Arrest 'Most Hated Man on the Internet' in Revenge Porn Hacking" *Arstechnica*, available at https://arstechnica.com/tech-policy/2014/01/feds-arrest-most-hated-man-on-the-internet-in-revenge-porn-hacking-case/ (visited 24 August 2019).

Gov.uk Press Release (2016) "New National Cyber Security Centre Set to Bring UK Expertise Together", available at www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together (visited 4 April 2019).

Greenberg A (2011) "HBGary Federal's Aaron Barr Resigns After Anonymous Hack Scandal" *Forbes*, available at https://www.forbes.com/sites/andygreenberg/2011/02/28/hbgary-

federals-aaron-barr-resigns-after-anonymous-hack-scandal/#646efce37591 (visited 4 April 2019).

Hackers Remotely Kill a Jeep on a Highway (2015) WIRED available at https://www.youtube.com/watch?v=MK0SrxBC1xs (visited 24 September 2021)

Internet World Stats (2021) "Internet user distribution in the world - 2021" available at https://www.internetworldstats.com/stats.htm (visited 24 October 2021).

Kaspersky Lab (no date) "Social Engineering Definition", available at https://usa.kaspersky.com/resource-center/definitions/social-engineering (visited 4 April 2019).

Kaufmann (2021) "Cyber attacks hit the City of Johannesburg and South African banks" available at https://www.thesslstore.com/blog/cyber-attacks-hit-the-city-of-johannesburg-and-south-african-banks/ (visited on 3 October 2021).

Khuthala (2013) "Corrective Rape: Lesbians at the Mercy of Powerless Men" *Mail & Guardian*, available at https://mg.co.za/article/2013-07-15-00-violence-against-black-lesbians-is-a-struggle-for-power (visited 4 April 2019).

Kilian (2017) "Cybercrime Becoming a Major Threat in South Africa" *Engineering News*, available at http://www.engineeringnews.co.za/article/cybercrime-becoming-a-major-threat-in-south-africa-2017-09-19/rep_id:4136 (visited 4 April 2019).

Leyden "Second Man Jailed over Scientology DDoS Attacks" *The Register*, available at https://www.theregister.co.uk/2010/05/25/second_scientology_ddoser_jailed/ (visited 24 August 2019).

Liebowitz (2012) "Cybercrime Gang Stole $5 Million in 72 Hours" *NBC News*, available at http://www.nbcnews.com/id/46044087/ns/technology_and_science-security/t/cybercrime-gang-stole-million-hours/#.WIiXqtJ97cs (visited 4 April 2019).

Toyana (2021a) "Cyber bandits target South Africa: Department of Justice, Space Agency hit by ransomware attacks" *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2021-09-09-cyber-bandits-target-south-africa-department-of-justice-space-agency-hit-by-ransomware-attacks/ (visited 20 September 2021).

Toyana (2021b) "Transnet ports division declares force majeure on container terminals after cyber attack" *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2021-07-27-transnet-ports-division-declares-force-majeure-on-container-terminals-after-cyber-attack/ (visited20 September 2021).

Morris (2012) “Hunter Moore: The Most Hated Man on the Internet” *Rolling Stone*, available at https://www.rollingstone.com/culture/culture-news/hunter-moore-the-most-hated-man-on-the-internet-184668/(visited 4 April 2019).

MrDevStaff (2016) “Petya Ransomware Demonstration” *YouTube*, available at https://www.youtube.com/watch?v=zOSI08mnfzM (visited 4 April 2019).

Murray (2012) “IsAnyoneUp? Shuts Down: 'Revenge Porn’ Forum Bought by Anti-Bullying Website” *NY Daily News*, available at http://www.nydailynews.com/news/money/isanyoneup-shuts-revenge-porn-forum-bought-anti-bullying-website-article-1.1064608 (visited 4 April 2019).

MyBroadband (2018) “SAPS Cybercrime Unit Crippled by Expired Software Licences” available at https://mybroadband.co.za/news/security/275703-saps-cybercrime-unit-crippled-by-expired-software-licences.html (visited 4 April 2019).

Namestnikov & Garnaeva (2012) “DDoS Attacks in H2 2011” *Kaspersky*, available at https://securelist.com/ddos-attacks-in-h2-2011/36535/ (visited 4 April 2019).

News24 (2012) “Johannesburg Taxi Rank Assault Condemned”, available at http://www.news24.com/SouthAfrica/News/Johannesburg-taxi-rank-assault-condemned-20120103 (visited 4 April 2019).

News24 (2015) “WATCH: Hacktivist Group Anonymous Joins us in Studio”, available at https://www.news24.com/Video/SouthAfrica/News/WATCH-Hactivist-group-Anonymous-joins-us-in-studio-20150205 (visited 4 April 2019).

News24 (2016) “Expect More Hack Attacks in SA – Anonymous” *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2016-07-25-expect-more-hack-attacks-in-sa-anonymous/#.W0sLAtIzZEY (visited 4 April 2019).

Norton (2011) “Anonymous 101: Introduction to the Lulz” *Wired*, available at https://www.wired.com/2011/11/anonymous-101/ (visited 4 April 2019).

Odonkor (2020) “Unveiling the cost of cybercrime in Africa” available at https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html (visited 30 September 2021)

Ott (2018) “What You Should Know about the 24/7 Cybercrime Network”, available at https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf (visited 2 January 2020).

Perez (2019) “To cut down on spam, Twitter cuts the number of accounts you can follow per day” Techcrunch available at https://techcrunch.com/2019/04/08/to-cut-down-on-spam-twitter-cuts-the-number-of-accounts-you-can-follow-per-day/ (visited 22 October 2021).

Rasch (1996) “The Internet and Business: A Lawyer’s Guide to the Emerging Legal Issues” *Criminal Law and the Internet,* available at http://groups.csail.mit.edu/mac/classes/6.805/articles/computer-crime/rasch-criminal-law.html (visited 2 February 2019).

Scheier (2007) “Dumpster-Diving for E-Data” *Computer World*, available at https://www.computerworld.com/article/2542491/dumpster-diving-for-e-data.html (visited 24 August 19 2019)

Schiffer (2019) “The life of a white-hat hacker” Vox Technology available at https://www.vox.com/the-highlight/2019/8/1/20742426/hacker-hacking-white-hat-ethical (visited 22 October 2021).

Security Trails (2018) “An Ode to White Hats: What is Ethical Hacking”, available at https://securitytrails.com/blog/ode-white-hats-ethical-hacking (visited 4 April 2019).

Ngqakamba (2021) “Justice Department’s IT system brought down in ransomware attack” *News24, a*vailable at https://www.news24.com/news24/southafrica/news/justice-departments-it-system-brought-down-in-ransomware-attack-20210909 (visited 30 September 2021).

Sharman (2017) “Cyber-Attack that Crippled NHS Systems Hits Nissan Car Factory in Sunderland and Renault in France” *Independent*, available at https://www.independent.co.uk/news/uk/home-news/nissan-sunderland-cyber-attack-ransomware-nhs-malware-wannacry-car-factory-a7733936.html (visited 4 April 2019).

Shugarman (2017) “Marcus Hutchins Arrest: Computer Expert who ‘Helped to End NHS Cyber-Attack’ Charged with Malware Offences in US” *Independent*, available at http://www.independent.co.uk/news/uk/home-news/marcus-hutchins-arrested-latest-us-authorities-wannacry-cyberattack-nhs-las-cegas-mccaran-a7875761.html (visited 4 April 2019).

Slownlow210 (2012) “Amanda Todd’s Story: Original Video by Her’ *YouTube*, available at https://www.youtube.com/watch?v=v2QRbl3H0ug&t=8s (visited 4 April 2019).

Smith (2019) “SA Civil Aviation Authority launches investigation into possible cyber hack” Fin24 available at https://www.news24.com/fin24/Companies/Industrial/sa-civil-aviation-authority-launches-investigation-into-possible-cyber-hack-20190708 (visited 3 October 2021).

Stack (2018) “Here’s How Much your Personal Information is Selling for on the Dark Web” *Experian Information Solutions*, available at https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (visited 4 April 2019).

State Information Technology Agency, available at http://www.sita.co.za/ (visited 24 August 2019).

Surbramaniam V & Whalen J (2014) “Dutch Man Suspected of Tormenting Amanda Todd had 75 other Victims, Facebook Report says” *CBC*, available at http://www.cbc.ca/1.2857281 (visited 4 April 2019).

Swart (2012) “It was a Happy New Year's Day for Gang who Pulled off … R42m Postbank Heist” *Sunday Times*, available at http://www.timeslive.co.za/local/2012/01/15/It-was-a-happy-New-Years-Day-for-gang-who-pulled-off...R42m-Postbank-heist (visited 4 April 2019).

Techopedia (no date) “What is Malvertisement?” available at https://www.techopedia.com/definition/4016/malvertising (visited 24 August 2019).

TechTarget (2017) “Botnet”, available at http://searchsecurity.techtarget.com/definition/botnet (visited 4 April 2019).

Temple (2013) “Limiting Intimate Posts Used as Revenge” *SF Chronicle*, available at http://www.sfgate.com/technology/dotcommentary/article/Limiting-revenge-porn-is-topic-of-legislation-4765856.php (visited 4 April 2019).

The Fifth Estate (2014) “Stalking Amanda Todd: The Man in the Shadows” *CBS News*, available at https://youtu.be/GRidpO7kUO0 (visited 4 April 2019).

Van Zyl (2016a) “Anonymous ‘Hacks’ Armscor Website” *Fin24*, available at https://www.fin24.com/Tech/News/anonymous-hacks-armscor-website-20160712 (visited 4 April 2019).

Van Zyl (2016b) “Expect More Hack Attacks in SA – Anonymous” *Fin24*, available at https://www.fin24.com/Tech/Cyber-Security/expect-more-hack-attacks-in-sa-anonymous-20160725 (visited 4 April 2019).

Vermuelen (2016a) “Anonymous Hacks and Leaks South African Government Data” *MyBroadband*, available at https://mybroadband.co.za/news/security/155278-anonymous-hacks-and-leaks-south-african-government-data.html (visited 4 April 2019).

Vermuelen (2016b) “This is How I Took Down the SABC: Anonymous Hacker” *MyBroadband*available at https://mybroadband.co.za/news/security/168303-this-is-how-i-took-down-the-sabc-anonymous-hacker.html (visited 4 April 2019).

W3Tech (2021) “Distribution of websites by server location” available at https://w3techs.com/technologies/overview/server_location (24 October 2021).

Walker (2013) “Man who Got Rich from 'Revenge Porn' Website UGotPosted is Finally Exposed” *Independent*, available at http://www.independent.co.uk/news/world/americas/man-who-got-rich-from-revenge-porn-website-ugotposted-is-finally-exposed-9001709.html (visited 4 April 2019).

Weisman (no date) “Dos Atacks Explained” *Symentec*, available at https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html (visited 4 April 2019).

White (2014) “On the Trail of Amanda Todd Alleged Tormenter” *The Globe and Mail*, available at https://www.theglobeandmail.com/news/world/on-the-trail-of-amanda-todds-alleged-tormentor/article18935075/ (visited 4 April 2019).

Reports and Theses

Australasian Centre for Policing Research & Australian Transaction Reports and Analysis Centre (2006) “Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency” *Report Series No 1453*.

Australian Bureau of Statistics (2012) *Personal Fraud Survey 2010–2011* No 4528.0.

Binational Working Group on Cross Border-Mass Marketing Fraud (2006) *Report on Phishing: A Report to the Minister of Public and Safety and Emergency Preparedness Canada and the Attorney General of the United States*.

Corrigan (2020) *Africa’s ICT infrastructure: Its present and prospects* South African Institute of International Affairs Policy Briefing 197.

Delaporte & Bahia (2021) *The state of mobile internet connectivity 2021* Global System for Mobile Communications (GSMA).

Europol (no date) “Wannacry Ransomware” available at https://www.europol.europa.eu/wannacry-ransomware (visited 4 April 2019).

Falk C (2004) “Gray hat hacking: Morally Black and White” *Centre for Education and Research in Information Assurance and Security Tech Report*.

Gercke M (2012) “Understanding Cybercrime: Phenomena, Challenges and Legal Response” *ITU Telecommunication Development Bureau Report*

Gumbi (2018) *Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom*, University of Cape Town (Masters Dissertation).

International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database (available at https://data.worldbank.org/indicator/IT.NET.USER.ZS?contextual=default&name_desc=false) accessed 09 September 2021

International Telecommunications Union (2009) "Understanding Cybercrime: A Guide for Developing Countries" *ITU-D ICT Applications and Cybersecurity Division*.

International Telecommunications Union (2013) "Big Data: Big Today, Normal Tomorrow" *ITU-T Technology Watch Report*.

Marsh (2017) *Are Ethical Hackers the Best Solution for Combating the Growing World of Cyber-Crime?* (Doctoral dissertation, University Honors College, Middle Tennessee State University).

Mcanyana, Brindley & Seedat (2020) "Insight into the cyberthreat landspace in South Africa" Accenture.

McGuire M & Dowling S (2013) "Cybercrime: A Review of the Evidence" *Home Office Research Report 75.*

Morris S (2004) "The Future of Netcrime Now: Part 1 – Threats and Challenges" *Home Office Online Report 62/04*.

Nakamoto (2018) "Bitcoin: a peer-to-peer electronic cash system" (independently published).

National Fraud Authority (2008) "The National Fraud Strategy: A New Approach to Combating Fraud" London: National Fraud Authority.

Pender-Bey G (2012) "The Parkerian Hexad: The CIA Triad Model Expanded" Thesis for Master of Science in Information Security Program, Lewis University.

Pender-Bey G (2019) "The Parkerian Hexad: The CIA Triad Model Expanded" Thesis for Master of Science in Information Security Program, Lewis University.

Savage K, Coogan P & Lau H (2015) "Security Response: The Evolution of Ransomware" White Paper Version 1 *Symantec.*

South African Banking Risk Information Centre (2017) “2017 Card Fraud Booklet” available at https://www.sabric.co.za/media/1448/2017-card-fraud-booklet.pdf (visited 31 July 2018).

South African Banking Risk Information Centre (no date) “419 Scam”, available at https://www.sabric.co.za/stay-safe/419-scam/ (visited 24 August 2019).

South African Law *Reform* Commission (2000) “Computer-Related Crime: Preliminary Proposals for Reform in Respect of Unauthorised Access to Computers, Unauthorised Modification of Computer Data and Software Applications and Related Procedural Aspects” *Discussion Paper 99, Project 108*.

State Security Agency (4 December 2015) “National Cybersecurity Policy Framework for South Africa” *Government Gazette No 39475*.

Tjong T, Koops E, Op Heij D, Silva K & Skorvanek I (2015) “Duties of Care and Diligence against Cybercrime” 7(2017) Tilburg Private Law Working Paper Series 1 – 120.

Turianskyi (2018) “Balancing Cyber Security and Internet Freedom in Africa”, Occasional Paper no. 275. SAIIA (South African Institute for International Affairs).

Turianskyi (2020) “Africa and Europe: Cybergovernance Lessons” Policy Insights 77, SAIIA (South African Institute for International Affairs).

United Nations Conference on Trade and Development (UNCTAD) (2013) Harmonizing Cyberlaws and regulations: The experience of the East African Community.

United Nations Office on Drugs and Crimes (2013) *Comprehensive Study on Cybercrime* New York: UN.

Wittes et al. (2016) “Sextortion: Cybersecurity, teenagers, and remote sexual assault”, Brookings Institution available at https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf (visited 12 October 2021).