# AN ANALYSIS OF CYBERCRIME INVESTIGATION BY DIRECTORATE FOR PRIORITY CRIME INVESTIGATION

By

WINDY BAWINILE MNGADI

submitted in accordance with the requirements
for the degree of

Master of Arts

in the subject

CRIMINAL JUSTICE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Dr DQ Mabunda

November: 2021

**DECLARATION**

I, Windy Bawinile Mngadi, student no. 43454771 declares the following:

- I understand plagiarism and what it entails, and I am fully cognisant of the policy that the University upholds.
- I declare this assignment to be my own original work and declare that where I have used somebody else's work (printed copies, Internet, interviews or any other source), I have acknowledged the authors, or the owners of such material, by means of comprehensive references as per the department's requirements.
- I declare that I did not copy and paste any information from any electronic source into this document.
- I did not submit another student's work as my own.
- I did not share or allow anyone to copy my work to submit as their own.
- I declare that all the obtained information of a sensitive nature has been treated with the confidentiality it deserves.

_____ 2021/11/14

Mrs W.B. Mngadi Date

**ABSTRACT**

Cybercrime has taken on epic proportions and it is rapidly becoming a major threat in South Africa; as technology evolves, similarly the cyber criminals become more innovative. The following problems were identified by the researcher during interviews conducted:

Investigations require adequate resources to investigate such crimes.

There is a need for continuous training to keep abreast of the ever-changing technology.

The lack of skills and knowledge required for investigating cybercrime.

The research design that was used in the study is a qualitative research approach. The sixteen research participants who met the requirements of the study were selected by means of purposive sampling. Interviews were used to collect data.

The aim of the study is to analyse the impact of computer crime in South Africa and determine whether detectives of the South African Police Service (SAPS) and Directorate for Priority Crime Investigation (DPCI) officials possess the relevant skills required to investigate cybercrimes.

Various literature reviews were consulted to gather information on other Authors' findings on this area of study.

**KEY WORDS:** Cybercrime, Computer crime, Digital crime, Legislation, Modus Operandi, Cyber-attack, Fraud.

**ACKNOWLEDGEMENTS**

First and foremost to God Almighty, I would like to express my deepest gratitude for His Grace that has carried me this far.

My sincere appreciation to the following people who made this study possible:

- The Department of Correctional Services: Pietermaritzburg Management Area and the South African Police Service in KwaZulu-Natal: Pietermaritzburg Cluster. Thank you, may God bless those hands.
- All the participants who were involved in this study, I appreciate your effort.
- Ms. Sizeni Makhathini, thank you very much for your invaluable advice.
- My families Mngadi and Ngcemu oNkayishane kaNonkenyeza. I appreciate the support you gave me.
- My husband Mngadi, Madlokovu, Ntusi, Ngema and the kids Aphiwe, Owethu and Asiphesona. Thank you so much for all the love and unwavering support you gave me throughout the study.
- My supervisor, Dr Mabunda, for believing in me and your unconditional support throughout this journey; I am yet to meet a more tolerant man. Thank you, Sir.

## LIST OF ABBREVIATIONS AND ACRONYMS

| | | |
|---|---|---|
| SAPS | : | South African Police Service |
| DPCI | : | Directorate for Priority Crime Investigation |
| DCS | : | Department of Correctional Services |
| FSL | : | Forensic Science Laboratory |
| UNISA | : | University of South Africa |
| MO | : | Modus Operandi |
| CSC | : | Community Service Centre |
| CRC | : | Criminal Record Centre |
| CR & CSM | : | Criminal Record and Crime Scene Management |
| CRIM | : | Criminal Record Information Management |
| CSI | : | Crime Scene Investigator |
| FIPS | : | Fingerprint Identification Profiling System |
| HANIS | : | Home Affairs National Identification System |
| LCRC | : | Local Criminal Record Centre |

## TABLE OF CONTENTS

## CHAPTER ONE: GENERAL ORIENTATION

### 1.1 INTRODUCTION AND BACKGROUND OF THE STUDY

South Africa is reportedly ranked number three in the world with regard to cybercrime. “Mercury (2018) reports that South Africa has the third highest figure of cybercrime victims global resulting in loss of about R2, 2billion each year to cyber-attacks. According to 2018 South African Banking Risk Information Centre (SABRIC) report”. Casey and Ferraro (2004:667) describe cybercrime as the means by which criminals manipulate readily available information in the public domain for their nefarious deeds to exploit unsuspecting victims. Cybercrime involves multiple Modus Operandi, thereby making it difficult to detect and investigate. Gillespie (2015:1) argues that cybercrimes is the subset of computer crime and this must be correct. Various authors define cybercrime in various ways, and it is for these reason that researcher in this study sought to dig deeper in order to come up with an easy to understand description. For this reason, authors such as Kumar (2009:28) point out that researchers must look at issues such as motives, behaviour in their attempt to describe or define the concept. For this reason, researchers should look at various definitions before crafting their own. This will ensure that relevance issues are sorted out because the time frame and context may have changed from the period when a concept was described. Furthermore Brits (2013:5) indicates that cybercrime has been traditionally defined as encompassed abuses and misuses of computer systems or computers connected to the internet which result in direct and/or concomitant losses.

Moreover, Steven and Gilbert (2013:3) says that the term cybercrime strictly speaking means “cyber” tends to deal with networking issues, especially including global networks, such as the internet. Similarly, Roddel (2011:1; Ncube, 2016:3; Sihori, 2015:18) defines Cybercrime as a crime where a computer or a computer network is a necessity tool to complete the crime or is the target of the crime.

Schell and Martin (2004:33; Helfgott (2008:401) explains that there are four elements of cybercrime for a property involving (1) criminal trespass, defined as entering unlawfully into an area for the purpose of committing an offense, and (2) theft of information or software - the intended offense to be done upon entry. However, Schell and Martin (2006: 83) point out that as in traditional crimes for a cybercrime to exist four elements need to be present: *actus reus* (the prohibited act or failing to act when one supposed to be under

duty to do so): *mens rea* (a culpable mental state): attendant circumstances (the existence of certain necessary conditions): and harm resulting to persons or property.

## 1.2 PROBLEM STATEMENT

Walliman (2016:73) defines a research problem as the general statement of a matter meriting research. Its nature will suggest appropriate forms for its investigation. However, DePoy and Gitlin (2016:56) point out that the identified research problem should lead to an inquiry that either yields new knowledge or verifies existing knowledge that is beneficial to the investigator.

Cybercrimes are increasing drastically and becoming major threats in South Africa. This statement is supported by the 2018 SABRIC Digital Banking Statistics Report indicating that “South African banks suffered a gross loss of 55% between January and August 2017, with 13 438 reported incidents of cybercrime”. For the period January to August 2018, 16 296 incidents had been reported reflecting a 19, 9% increase in cybercrimes, compared with the same period the previous year (2017). Moreover, the SAPS Annual Report of 2016/2017 indicated a total of 11 395 reported cases of commercial crime in the Province of KwaZulu- Natal, for the period 2015/ 2016 and 12 405 reported cases for the period 2016/ 2017. “These statistics show an increase of 1 010 reported cases translating to an increase of 8.8% year-on- year”.

The Sicesha Report (2018) has revealed that the Cybercrime Unit of the South African Police Service (SAPS) is unable to function and investigations into organised crimes, hacking and EFT scams have been halted due to expired software licenses. They also make use of contractors to assist in the investigation. As Van Rooyen (2008:03) explains, we cannot deny the fact that investigators are facing huge challenges in South Africa as cybercrimes are on the rise. Van Rooyen further argues that most cybercrime goes undetected as officers assigned to investigate these kinds of crimes, do not possess specific knowledge and skills. In addition, Cross (2008:94) believes that although the cybercrime phenomenon has grown in recent years, many information technology (IT) and law enforcement professionals lack the necessary tools and expertise to address the problem of cybercrimes. Furthermore Cassim (2011:125) said cybercrime differs from traditional crime. It can be committed easily; it requires a few resources and it can be committed in a specific area without the offenders being physically present there. Moreover, Schmalleger (2005:760) points out that the fact that advances in technology

over the past years including computer networking, the internet wireless services have ushered in a wealth of new criminal opportunities. According to Security Company (2016), almost 9 million South Africans have been victims of cybercrime. Furthermore, Hawks (2017) pointed out the incidence of approximately 43% of card fraud between January and September 2017. In addition, Serrao (2017) states that personal data of more than 30 million South Africans had apparently been leaked online.

## 1.3 RESEARCH AIM AND OBJECTIVE

The purpose of this study is to analyse the impact of computer crimes in South Africa and determine whether the South African Police detectives possess the relevant skills required to investigate cybercrimes.

- The research objectives were: To analyse the impact the cybercrime in South Africa
- To determine the procedures and techniques that were used when investigating cybercrime was still effective as cyber criminals are advances on daily basis.

## 1.4 KEY THEORETICAL TERMS

### 1.4.1 Cybercrime

According to Brits (2013:5) cybercrime is defined as any criminal act committed via computer. In addition, Chawki, Darwish, Khan and Tyagi (2015:3) define cybercrime as unlawful acts wherein the computer is either a tool or target or both.

### 1.4.2 Computer crime

Franklin (2006:8) defines computer crime as any crime involving a processing unit or computer.

### 1.4.3 Digital crime

Brits (2013:5) defines digital crime as any criminal activity which involves the unauthorised access, dissemination, manipulation, destruction, or corruption of electronically stored data. However, Steven and Gilbert (2013:4) define digital crime as crime directed at a computer or a computer system.

### 1.4.4 Cyber security

Edgar and Manz (2017:34) define cyber security as the act of making cyber space safe from damage or threat.

### 1.4.5 Legislation

Gilmore (2014:14) refers to Legislation as the law that comes from parliament. Bills are put before parliament and if, or when they are passed, they become Acts and then enforce law as from their respective commenced dates.

### 1.4.6 Cyber attack

According to Russell (2014:8) cyber-attacks can be defined as deliberate actions to alter, disrupt, deceive, degrade or destroy computer systems or networks or the information and or programmes resident in or transiting these systems or networks.

### 1.4.7 Fraud

Turner and Weickgenannt (2009:80) define fraud as theft, concealment and conversion for personal gain of another's money, physical assets or information.

## 1.5 RESEARCH QUESTION

"The research questions are the critical part of the researcher's proposal". They guide the researcher's arguments and provoke the interest of the reader.

### 1.5.1 What is the impact of computer crimes in South Africa?

The research sub-questions are as follows:

- What is a cybercrime?
- Who are the victims of cybercrime?
- How does cybercrime affect the victim(s)
- What was the impact of cybercrime on the South African community?
- How does the police investigate cybercrime?
- The modus operandi of Cyber criminals or offenders
- How can investigators be skilled in cybercrimes?
- What was the legislation that guides cybercrimes in South Africa?
- How do we curb cybercrimes in South Africa?

## 1.6 RESEARCH METHODOLOGY

Quinian (2011:482) defines research methodology as the signals to the reader how the research was conducted, scientific methods and the philosophical assumptions underpin the research. However, Creswell (2007:139) argues that research methodology is the

systematic, theoretical analysis of the methods applied to a field of study. Typically, it encompasses concepts such as paradigm, theoretical model, phases and quantitative or qualitative techniques. In addition, Kumar (2008: 05) explains that research methodology is a way to systematically solve the research problems. It may be understood as the science of studying how research is done scientifically.

The researcher adopted qualitative technique when conducting this study by conducting interviews to Police Detectives and DPCI Officials.

### 1.6.1 Research design

Le Compte and Schensul (2010:87) explains that research design is a detailed set of questions hunches which produces a plan of action for the conduct of a research project. Moreover, Van Wyk ([sa]:3) said that research design is the overall plan for connecting the conceptual research problem to the pertinent and achievable empirical research. In other words, the research design articulates what data is required, what methods are going to be used to collect and analyse this data, and how all of this is going to answer your research question, both data and methods, and the way in which these will be configured in the research project. However, Kumar (2019:95) says that research design is a plan, structure and strategy of investigation so conceived as to obtain answers to research questions and problems. In addition, Cooper and Schindler (2014:125) define research design as an activity and time based. Research design involves the following:

- A plan based on the research question;
- A guide for selecting sources and type of information;
- A framework for specifying the relationships amongst the study variables;
- A procedural outline for every research activity.

Research design is the plan, structure and strategy of investigation conceived to obtain answers to research questions and control variance. Cauvery, Sudha, Nayak, Girija, and Meenakshi (2003:49) point out that research design provides a framework for collection and analysis of data. Moreover, De Vos (2002:120) describes Research design as the blueprint of a detailed plan the research has to follow conducting operationalising variables so that it could be measured, selected sample to the study, collecting data and analysing the results. In addition, Bryman *et al*., (2011:100) define research design as the framework for collection and analysis of data. Similarly, Krishnaswamy, Sivakumar and

Mathirajan (2006:22) describes research design as a multidimensional concept. It is a plan of research to determine the type of research, measurement method, and types of sampling, data collection methods and method analysis. Research design relates directly to the answering of research questions (Bless, Higson-Smith and Sithole, 2013:130).

The researcher agrees with De Vos (2002) and Bless *et al*., (2013:130) that research design is the set of methods and procedures used in collecting and analysing measures of the variables of specified in the research problem and to answer to research questions

The researcher will use qualitative methods in this study by conducting interviews with Police Investigators in Pietermaritzburg Police Stations and DPCI (known as Hawks) Personnel.

### 1.6.2 Population and sampling

The researcher will conduct the study in the Province of KwaZulu-Natal, more specifically, Pietermaritzburg Police Station Clusters and DPCI Section. The researcher will use purposive sampling in this study. Babbie and Benaquisto define purposive sampling as a type of non-probability sampling in which one selects the units to be observed on the basis of one's own judgement which will be the most useful or representative. Another name for purposive sampling was judgemental sampling. Furthermore, Neuman (2014:169) explains that purposive sampling is a valuable kind of sampling for special situations. It was usually used in exploratory research or in field research. In this type of sampling, the judgement of an expert or prior knowledge is used to select cases. Kumar (2011:178) argues that sampling is the process of selecting a few samples from a bigger group to become the basis for estimating or predicting the prevalence of an unknown piece of information.

Cooper and Schindler (2011:160) explains that qualitative research includes an array of interpretive techniques, which seek to describe, decode, translate and otherwise come to terms with meaning. To understand the different meanings that people place on their experiences often requires research techniques that delve more deeply into people's hidden interpretations, understandings and motivations. Qualitative research is the collection and analysis of primarily non-numerical data (words, pictures and actions). (Bryman, *et al*., 2011:41).

Bless *et al*., (2013:394) define population as the set of elements (unit analysis) that the researcher focuses upon from which the results are obtained. In addition, Blankenship (2010:82) explains that population is the group of all individuals, organisations, or artefacts that could be involved in the study. The population is also the group that the researcher wants the results of the study to apply to at the conclusion of the study. Furthermore, Babbie and Benaquisto (2010:108) point out that the population of study is the group (usually the people) about whom we want to draw conclusions.

The research will conduct interviews with Police Investigators. Pietermaritzburg Police Stations (such as Pietermaritzburg, Prestbury, Alexandra, `Townhill) and Pietermaritzburg DPCI Section. The researcher opted for this group because these police stations are the big and busy police stations in Pietermaritzburg. The research intended to interview all the investigators in those identified police stations.

## 1.7 DATA COLLECTION

Welman, Kruger and Mitchell (2005:127) argue that collected data must only be used for a particular purpose and thereafter either archived appropriately or safely disposed. This will ensure that such data do not end up in wrong hands or inadvertently expose participant to any form of prejudice or harm. For this reason, it is important that researchers design questionnaires or any method they intend to use in data collection bearing in mind the ultimate objective. In this research, the researcher aimed to interview investigators who have first-hand knowledge and experience in cybercrime investigation. This can be evident when one look at participants' responses verbatim in the interpretation and analysis section. This view is supported by (Eadie, 2009:186) who argues that, information obtained from participants in the interview must solely be used for an intended purpose. This means that using obtained data for ulterior purposes border on academic and ethical dishonesty, a consequence which should be avoided at all costs. Moreover, (Hakim, 2000; Anderson and Arsenault, 2005:190; Seidman, 2006:10) are of the view that questions asked during interviews should be directly related to the objectives of the study, which is what the researcher in this study managed to achieve.

The researcher will use interviews and field notes in collecting the data. The aim of this approach is to ensure that each interview conducted presents the same questions and in the same order. It is much easier, and time is limited to conduct interviews especially in the busy schedules of the police investigators and Bank personnel. Kumar (2014:177)

defines interview as the verbal interchange, often face to face, though the telephone may be used, in which an interviewer tries to elicit information. In addition, Gubrium, Holstein, Marvasti and McKinney (2012:15) said an interview is a conversation or questioning for the purpose of eliciting information for publication. The researcher will obtain data through interviewing and questionnaires.

### 1.7.1 Literature Review

Jesson, Matheson and Lacey (2011:10) defines a literature review as a written appraisal of what is already known as existing knowledge on a topic. In addition, Machi and McEvoy (2012:04) explain that a literature review is a written document that presents a logically argued case founded on a comprehensive understanding of the current state of knowledge about a topic of study. Similarly, Kreuger & Neuman (2006) are of the opinion that a literature review is a synthesis on a topic. Creswell (2005) goes into detail in noting that a literature review involves locating summaries, books, journals and indexed publications on selective topics, choosing which literature to conclude in your review and summarising the literature to include in your review. According to Ndara (2016) the problem encountered by researchers was that the South African Police Service Cybercrime Unit is seizing computer evidence. The following problems were identified by the researcher in practice: evidence was destroyed or lost because of mishandling by investigators, computer evidence was often not obtained or recognised due to a lack of knowledge and skills on the part of investigators to properly seize computer evidence.

According to Hart (2002:02), the importance of the search for a literature review is the essential part of every research project. There are two areas to be searched when you are beginning a research project.

- The literature relevant to the topic.
- The literature on research methodology and data collection techniques.

Hart further argues that an analytical reading of literature is an essential prerequisite for all research. It is especially important to have read the literature if you aim to collect raw data. Furthermore, Aveyard (2014:04) explains that literature reviews are important because they seek to summarise the literature that is available on any topic. They make sense of a body of research and present an analysis of available literature so that the reader does not have to access each individual research report included in the review. In

addition, DePoy and Gitlin (2013:45) point out that one important purpose of reviewing the literature for research is to help sharpen focus of your initial research interest and the specific strategy you plan to use to conduct a study. Discovering what others know and how they come to know it is an important function of the review when conducted at the initial stage of developing a research idea.

Dlamini & Mbambo (2013:2) points out that online fraud in South Africa remains the top 5 attacked countries in the world in terms of phishing attacks discovered in September 2011. In addition, Gubrium *et al*., (2012) noted that the international scope of the internet and the increase in cyber-attacks the South Africa administrative and legislative system to both intersect largely with the application and implementation of international legislation. Furthermore Stander, Dunnet and Rizzo (2009) says that the internet provides endless connectivity to billions of users around the world which has greatly influenced the flow of information. As revolutionary as this has been, the associated benefits have extended to the criminal world and allowed these miscreants to take advantage of this powerful tool to commit a host of computer crimes. Ndara (2013) points out that the threat of cybercrime on computer systems has become a global economic issue; developing countries such as South Africa, Zimbabwe and Nigeria are often the target of cybercrimes due to their weak security measures. In South Africa, the National Cyber Security Hub (CSIR 2016) reported that there were 6000 attempted cyber-attacks against South Africa's critical infrastructure, business and Internet service providers between 2011 and 2015. Linda (2013) explains that in the United States in 2015, the internet Crime Complaint Centre of the Federal Bureau of Investigation (FBI) reported that 288,012 complaints of internet crime were received and more than $ 1 billion was lost to such crime that year alone. Criminals are committing traditional and high-tech crimes using their own computers, smartphones and tablets. According to the Bureau of Justice Statistics, in 2014 an estimated 17.6 million people in the United States were victims of at least one incident of identity theft.

## 1.8 ETHICAL CONSIDERATIONS

Bless et al., (2013) define research ethics as the word derived from the Greek word *ethos* meaning one's character or disposition. It is related to the term morality, derived from the Latin term *moralis*, meaning one's manner or character. A moral issue is concerned with whether a behaviour is right or wrong, whereas an ethical issue is concerned with whether

the behaviour conforms to a code or a set of principles. Moreover, Hennink, Hutter and Bailey (2011:62) explain that the research studies are required to undergo formal assessment by an institutional review board to assess whether the research will be conducted ethically. The principles of ethical conduct of research are now well recognised.

Bryman *et al*., (2011:377) describe ethics as the study of morals and moral behaviour. Bryman further argues that ethics code is a set of moral prescriptions for researchers to follow. In addition, Wallace and Van Fleet (2012:68) stated that ethics is: (1) a general pattern or way of life; (2) a set of rules of conduct or moral code and (3); inquiry about ways of life and rules of conduct. The first definition is one most commonly used in everyday life. The study of ethics, an academic or philosophical area of interest, has tended to focus on the third edition definition. Traditional approaches to the study of ethics consider defining value systems by distinguishing between good and bad at a broad level based on the principle of fundamental issues of morality and judgement.

### 1.8.1 The UNISA policy on research ethics (2016) UNISA is committed to:

- Undertaking and promoting research that aims to benefit the people of South Africa and or beyond its borders
- Being guided by integrity, accountability and rigour in research
- Maintaining an environment for researchers in which they are autonomous, yet ethical in their research practice
- Enabling researchers to maintain ethically responsible research practice.

### 1.8.2 Right to privacy, Anonymity and Confidentiality

The Constitution of the Republic of South Africa, 1996 provides the right to privacy, among other rights. It is therefore important that researchers respect these rights while conducting their research. Ignorance of the law is not an excuse; therefore, researchers will not claim to have been ignorant when participant indicate that researchers did not explain certain aspect while conducting research. It was therefore important that as the researcher, I explained what was required from participants. Moreover, participants' identities remained anonymous, as they indicated that due to the nature of the research, they would not like to be identifies for fear of victimisation later.

### 1.8.3 Informed consent

POPIA Act 4 of 2013. was adhered to, while conducting this research. Moreover, consent form was signed by all participants based on mutual trust. Where there is no consent, researchers are advised not to proceed, as doing so may invalidate or compromise the research. It is therefore significant that in instances where participants indicate their unwillingness or in some way feel uncomfortable, researchers must be mindful and make other legal or acceptable ways to obtain required information. In this research all participants signed consent forms and agreed to participate. The researcher obtained necessary permission from participants after they were thoroughly informed about the purpose of the interview. The researcher conducted the study in KwaZulu-Natal, Pietermaritzburg Police Stations with Police detectives. The researcher also obtained Ethical Clearance form UNISA to conduct this study.

## 1.9 SUMMARY

This Chapter presented the general orientation, focusing on introduction and study background, study rationale, problem statement, the study aim, objectives and research questions, research design and methodology, definition of key terms that guided this study, as well as the study significance. Ethical consideration aspects were also presented. The next chapter (two) will be the literature review.

## CHAPTER TWO: LITERATURE REVIEW

### 2.1 INTRODUCTION

Cybercrime is explained by Jaishankar and Ronel (2013: 404) as the use of computers and the internet by lawbreakers to perpetuate fraud and other crime against companies and customers. It is used to describe criminal activities committed on the computer or internet. However, Ross (2009: 18) defines cybercrime as sometimes used to mark activities in which offenders utilize computers or other electronic IT devices to ease illegal behaviors via data systems. Cyberspace can be outlined in terms of three layers: logical network, physical network as well as cyber-persona Van Puyvelde, 2019; Broadhurst**,** 2006). To this finale, these authors argue that in cybercrimes, there are huge numbers of possible victims, as well as unauthorised access, damage and intervention to computer systems. Chambers-Jones and Hillman (2014: 39) further point out that cybercrime is recognised as a criminal act committed using automatic communications networks and data systems or against such networks and systems. The European Commission therefore proposed three-fold definitions:

- Traditional forms of crime including fraud or forgery, perpetrate over electronic communication networks and data systems;
- The periodical of illegal content over automated media such as incitement to ethnic hatred; and
- Crimes distinctive to electronic networks such as strike against data systems or services or hacking.

Moreover, Chawki, Darwish, Khan and Tyagi (2015: 3) says that the term cybercrime is any criminal activity that involves a computer either as a target, an instrument or means for perpetuating further crimes comes inside the scope of cybercrime. A generalised explanation of cybercrime may be illicit move wherein the computer it might be a tool or target or both. Strictly speaking things “cyber” tend to deal with networking subject, including global systems, for- example, internet. Moskowitz (2017: 3) said one of the record persistent situations facing the digital world in the 21$^{st}$ century is cybercrime. The costs knowledgeable with the non- success of computers and other electronic devices to deter cybercriminals from destructive and gradually sophisticated occurrences are truly huge and growing promptly. In addition, Bidgoli (2004: 326) defines cybercrime as the unlawful act, committed by system of computer networks that can be consummate while

sitting at a computer keyboard. Such acts comprise of gaining illegal access to computer documents. Furthermore, Singh and Bakar (2019) define cybercrime as the crime committed in cyberspace through tools such as computers and smartphones using network systems intending to violate confidentiality.

The researcher defines cybercrime as an unlawful and intentional act to conduct criminal activity by means of computer or electronic network.

## 2.2 THE MODUS OPERANDI OF CYBERCRIME

Reddy and Minnaar (2018) explains that Cryptocurrencies are dominant in South Africa and get as far as traction as another online currency. Due to the unregulated and pseudo-anonymous nature Cryptocurrencies are also founding themselves as an ultimate currency for cybercriminals. Cryptocurrencies can be used as a target or tool in the aid of cybercrimes, such as capitalising scams, cyber fraud, hacking, phishing, cyber extortion and other financial crimes such as Ponzi as well as cyber money laundering. Criminologists should have a basic knowledge of the criminal conduct of crypto currency crime.

Furthermore, Schell and Martins (2004: 33) emphasise that there are four elements of involving cybercrime:

(1) Criminal trespass, defined as unlawfully entering into an area for the purpose of committing an offense;
(2) Theft of information or software - the intended offense to be done upon entry;
(3) A culpable mental state;
(4) A prohibited result or harm.

Furthermore Helfgott (2008: 401) says that there are four main elements of cybercrime namely: Location, Victim, Offender and the Action. (1) Location of the offender in relation to the crime: the criminal is usually not present at the scene of incident (2) Victim: Key victim is usually a government Institutions; corporation, organisation, people are also victims. (3) Offender: Cyber offenders are a heterogeneous group, including youngsters who are experimenting for fun; adults attempting to steal crucial data; individuals and groups involved in software copy illegally and illegal transfer who are not aware they are committing online crime. (4) The act has taken to disregard the risk. Minnaar (2019) explains that cyber-attacks via malware, spyware and ransomware infection have

become common internationally. Ransomware has since 2013, become one of most malicious, damaging and prevalent of the many strains of malware used by cybercriminals. Firmly speaking, ransom is malware (malicious software) utilising the crime ware to hack into databases in order to lock down database records, so that the operator (target victim) is incapable to access the data files unless they pay a ransom. In other words, they are blackmailed to compensate up by worries of either liberating the 'apprehended data, trade it on the darknet to the highest bidder or the cybercriminal ransomers using private data to hack into operators banking accounts to rip-off funds from those illegitimately accessed accounts. If a victim (individual or organisation/company) refuses to pay such ransom, the documents are either permanently tamper-proof or infected with a malware computer virus, thus rendering future operation of the company or individual target difficult or almost impossible. Later more sophisticated forms of ransomware using encryption appeared in 2006 but this too became more innovative with ransomers requesting for a larger sum of money. This ransomware using ever more complex encryption formats, became known as crypto-ransomware and is a more current and dangerous development by cybercriminals. New schemes are continuously being dreamed up by cybercriminals who quickly realised that individual are willing to pay hundreds, if not thousands in ransom (usually using the cryptocurrency Bitcoin as the medium for payment) to have their stolen (locked) data released.

Minnaar (2016) said that cybercrime is not a new method of organised crime in that the offenders have just become more organised as an online network or group of crooks that cooperate in the unlawful underground black market by marketing stolen data, hiring out crime ware and even given that technical backup services for the determines of online crimes. There is no doubt that online criminals within the cybercrime environment have been more sophisticated in making use of malicious software so called malware in their attacks in cyberspace for the main motive of individual financial gain. Cybercriminals have developed and using a stronger malware that has evolved and changed into given that stealthier and more hidden malware such as malvertisement, iFrame script inject and ransomware. All of which have developed more problematic to identify and therefore, to combat.

The researcher explains that there are four elements of cybercrime (1) illegal with intention to trespass or to commit crime by means of computer (2) theft of data with

intention of personal gain (3) culpable mental state to conduct crime (4) with intent to harm. In addition Kempen (2019) said if each individual who has fallen victim to cybercrime reported it to the police, it will offer interesting figures regarding the number of people who have actually fallen victim to cybercriminals, cybercrime occurrences range from fraudulent credit card transactions to recognize theft when fraudsters attain credit in somebody else's name without a permission. It only becomes apparent for many people, when they are knowledgeable about unresolved debt for something that was fraudulently funded in their name or when they are blacklisted. Other individuals might have been well alert of being victimised following a ransomware attack on their computer or due to an online scam.

Cybercrime can also comprise violent acts such as sexual crimes or terrorism attacks that are planned and culprits on the dark web, the list is endless. The question is whether authorities across the world can successfully recognize, investigate and deter the attack of this current crime phenomenon. The more significant question to enquire the South African Government and mostly the South African Police Service (SAPS), prepared to tackle cybercrime? Ezeji, Olutola and Bello (2018) says that cybercriminals utilises cyber-attack strategy such as viruses that attach themselves to normal files and malicious software, consequently reproducing themselves to cause damage to network or a computer system. Other strategy such as worms, backdoor programmes and Trojan are also utilised to reach entry to a computer system or network. Viruses and malicious software can also be moved by cybercriminals. Other related cybercrimes in South Africa such as e-commerce fraud and identity theft, involve the use of email or web pages to convince victims to reveal their personal or financial information. Furthermore Alazab and Broadhurst (2017) explain that the emergence of the internet of things (IoT) and the continued rapid growth of the internet have resulted in increased sophistication of malicious software, or crime-ware tools as well as the refinement of deceptive methods to conduct computer attacks and intrusions.

Cyber-attacks through spam emails (unsolicited bulk messages) remain one of the major vectors for the dissemination of malware and many predicate forms of cybercrime. Monitoring spam as potential cybercrime can help prevention by observing changes in attack methods including the type of malicious code and the presence of criminal networks. In addition, Nair, Dube and Lefophane (2017) emphasises the fact that Internet

of things (IoT) is predicted as a transformative approach that issue any service over the internet by enabling communications through the interconnection of heterogeneous devices. The possible attacks against IoT devices and potential threats have grown drastically and the cybercrime statistics from South African Banking Risk information reflect that South Africa loses in excess of R2,2 billion as a result of the security vulnerabilities annually. Unfortunately, the security requirements are not yet well addressed as it is at an infant stage. Sissing (2013) explains that the introduction of cyber technology, accompanied by fast expanding nature, has not only resulted in countless advantages to its user and society as a whole but has also produced harmful conditions specially impacting on cybercrime. One of these harmful effects is cyber stalking. The public as well as private individuals should therefore always remain vigilant against cyber stalking. Cyber stalking is defined as the use of internet or any electronic medium to stalk, pursue and harass victims. This unwanted perusal has various negative implications for the victim, as cyber stalking can disrupt many aspects of an individual's lifestyle.

In the same vein, Nel and Burger (2017) warns about the credit card skimming (electronic system of illegally capturing a victim's personal particulars by fetching data from the magnetic stripe of a credit or debit card) which has become a major worry in South Africa. As a result, these kinds of scam, millions of Rand are being stolen from both private and public entitles on a yearly basis. Cybercriminals utilises handheld card skimmers and position similar devices on Automated Teller Machine (ATM) to steal credit card data. Lately the use of compromised Point of Sale (POS) devices, that are used to illegally obtain the credit card information of unsuspecting card users in South Africa has increased rapidly (Shandu *et al.,* 2019*)*. It is also important to note that cybercriminals do not rest, and they continue tirelessly to crack password codes. Therefore, it is important for consumers to ensure that they do not create simple passwords such as using ones birthday dates. Shandu *et al*., (2019) warns that the public must also take precaution when they file their tax returns as this can also create an opportunity for cybercriminals to commit income tax fraud.

The South African law enforcement cybercrime unit experienced problems with confiscated, compromised POS devices. In order to decrypt the information, it was essential to obtain the unique password from the cybercriminals, something they were reluctant to reveal. To speak this delinquent, it was crucial to investigate the specific POS

device and associated with encryption/decryption software to find a technique to decrypt the information on the POS device without entree to the cybercriminal's unique password. Shandu, Maluleke and Lekgau (2019) said in South Africa income tax is unescapable, since all are accountable to pay taxes. Electronic filing (e-filing) was firstly introduced in 2001 and stretched out in 2006. However, the institution of e-filling generated opportunities for commission of income tax fraud. Tax fraud is explained among other illicit acts, as when a taxpayer defrauded tax deducted from other expenditures made to a creditor.

Gokhale (2020) explains that for almost years now, there have been some research attempts towards deploying open-source and designing, trustworthy and well-grounded systems that warrant operation by hiding the true network individuality of collaborating parties against overhearing opponents. TOR (The Onion Router) is an example of such systems. The implementation of TOR allows individuals to access the dark web, an area of the internet said to be of a much larger magnitude than the surface web. The dark web has earned a connotation with terrorist groups, child pornography human trafficking and hacking dark web research has received significant national and international press coverage. Moreover, currently little or no research has been showed on the illegal usage TOR usage by South Africans.

The researcher agrees with the researchers that there are number of cybercrimes modus operandi in South Africa such as new crime Cryptocurrency (Ponzi and investing scams). South Africans has invested in scams such MMM which later collapsed in 2016. "Alleged SA Ponzi scheme MMM's global pyramid collapses' Fin 24,04: 2016 explains that the Bitcoin based MMM Global Republic of Bitcoin scheme has collapsed, affecting the local branch in South Africa.

## 2.3 THE IMPACT OF CYBERCRIME ON THE SOUTH AFICAN COMMUNITIES

The impact of cybercrime in South Africa cannot easily be measured in terms of financial loss as it results in Millions if not Billions annually. Counting the cost is exacerbated by the fact that most victims do not even bother to report these crimes to the police, Mansell and Hwaang (2015: 117). Van der Waag- Cowling and Leenen (2019: 237) explained that the growth of the internet has improved how individuals and organisations conduct daily operations. From online banking to fitness apps. The internet has penetrated every aspect of our lives. Unfortunately, the growth and use of the internet produces many threats to

users. The evolution of the internet along with its various segments, has allowed cyber criminals to perform illegal e-commerce business such as transitional money (digital currency) laundering, selling of counterfeit and/or stolen goods compromises banking information, specially crafted malware. The entry of the taxonomy was proposed by the Council of Europe Convention of Cybercrime (The Convention was open for signature in November 2001 and came into force in July 2004). This taxonomy in particular is influential because the Cybercrime Convention was the first International treaty to specifically address the problem and a number of non-member states have also signed the Convention. These conventions include the United States, Canada, Japan and South Africa. The Convention has also had a significant impact outside boundaries of the signatory parties so called indirect impact or implementation becoming an International reference standard in the field of cybercrime.

Mercury (2018) reports that South Africa has the third highest figure of cybercrime victims global resulting in loss of about R2, 2billion each year to cyber-attacks. It is therefore evident that cybercrime and online fraud are the biggest challenge in cyberspace for different organisations, such as the Banks, Government institutions and individuals. However, Dlamini and Mbambo (2019) said computer crimes such as hacking showed great extension during the 90's in South Africa, because the internet became a popular way for users to connect worldwide. They further explained that the internet is one of the major scandals in contemporary society. It has become a symbol of technological ingenuity and has offered humankind the greatest of benefits, while on the other hand it may bring pain to a lot of people. For this reason, the researcher argues that the system must be put in a place to protect communities from potential cybercriminals. Such system must be capable of securing or protecting citizens from hackers or cyber criminals. In order for South Africans to have safe and secure cyberspace that is free from hackers, there needs to be a co-operative system put into place by the South African Criminal Justice System that involves the government, non-profit organisations and community.

Furthermore, Bougaardt and Kyobe (2011) said the level of cyber-attacks on structuring has increased extensively in recent years. When such attacks occur, organisations need to assess the damage and loss from this crime. However, these authors do not provide guidance for private individuals, which leaves private individuals exposed and having to devise their own survival means. While huge groups have the mechanisms to discover

such losses, private individuals lack such potential. SMEs lack such capability and usually ignore the necessity to implement actual information security measures. Olu (2020) explains that cybercrime and the project of the underground cyber economy have harmful consequences for the growth, and wellbeing of individuals, groups, organisations and nations of the world. Criminal activities such as hacking, scams, identity theft, fraud and cloning of individuals, corporate bodies and nations are attempts by cyber criminals to illicit scoop funds out of these several treasures for personal use. The underground cyber economy is a key factor that has strengthen the continued perpetration of cybercrime project. The study examines the underground cyber economy and its implications for the development of Africa.

Moreover Van Niekerk (2017) said the cyber security unsettle are present in everywhere but the exact nature of the warning differs depending on the country. Therefore, there is essential to assess the fears and impacts for particular countries. This article presents a high-level analysis of cyber incidents that affected South Africa. It was established that the most mutual impact type was data exposure, which was also one that had increased remarkably in current years. The most prevalent culprit type was established to be hacktivists, which had also revealed a recent escalation in activity. An extremely regarding trend was the recent high number of episode of data exposure caused by error, a trend moving contrary to the drive to improve cyber security. Desai (2018) says that this study uses the recent cyber-attacks on one of South Africa's largest financial institutions, Liberty Holdings, as an entry point to illustrate the encounter of cybercrime for the boardrooms of vast capital in South Africa. This violation reinforces arguments raised for strengthening the state's capacity to police cybercrime.

This research also reveals on the argument around the policing of cybercrime in South Africa, emphasising opinions that the way in which the state challenges to covenant with this increasing difficult has also formed qualms of the emergence of a surveillance state with unregulated powers lodged in intelligence agencies. This debate has been sharpened by current exposes of corruption seemingly endemic to South African intelligence services. Furthermore Malapane (2019) explains that globally online crime is on rise with cybercrimes expected to rise. This study is presenting a risk analysis of the online spending e-commerce in South Africa. It further outlines perceived risk of categories impact type, attacks vector and threat type. The outcomes of this study are

to present the risks related with finance losses impact online spending on e-commerce space. This has not yet been fully realised in South Africa. The next section present investigation of cybercrime.

## 2.4 HOW DOES THE POLICE INVESTIGATE CYBERCRIME?

Crime investigators worldwide are overwhelmed as crime continues to increase exponentially. There are various reasons why crime keeps rising, such as the level of unemployment and other socio-economy crime. However, research indicates that cybercrime is not necessarily committed by individuals who experience lack, but it is often largely associated with greed and malice (Dlamini and Mbambo (2019)). These authors argue that cybercrime is usually perpetrators who range from 18 to 35 years. According to Dlamini and Mbambo (2019), the challenge of investigating cybercrime in South Africa continues increasing year by year, making it big challenge to for police officials to keep up pace. Policing cybercrime requires highly experienced police officers who are not only better resources but keep on up skilling. Investigating and/or policing cybercrime is almost an impossible for many police organisations worldwide. Limited budget for policing leads to agencies prioritising resources for other issues rather than policing in general (Dlamini and Mbambo (2019)). Since cybercrime is borderless, police agencies require budget to enable investigators to criss- cross the globe in their endeavour to apprehend criminals and bring them for trials before court. The researcher argues that Interpol should be tasked with managing resources to investigating cross border crimes, using various sophisticated ICT better than the ones used by criminals. This requires a huge investment and commitment from all police agencies around the world. At this stage, cyberspace control is the battle ground for various network/syndicates. As a result, another difficult task for law enforcement for law enforcement is tracing cybercrime. The risk of cybercrime grows so does the challenge to police it. In addition, Montesano (2019) said as the technology advances and the availability of criminal services on the internet grows, the job of digital forensics investigators become more challenging. This challenge is increased when cyber criminal's utilise anti-forensic tactics, techniques and procedures (TTP's) to hide or delete evidentiary files or attempt to mislead or derail investigators. When anti-forensic TTP's are utilised by cyber criminals, several problems may arise. The digital forensic investigators may not be able to compile enough evidence to determine an accurate assessment of the situation in question when data is hidden or deleted. When

facing anti-forensic TTP's which attack the investigation process specifically, the validity of the investigations themselves may be called into question.

The policing of cybercrime is generally an afterthought for numerous organisations and individuals in South Africa. This type of crime has no boundaries. This contributes towards the challenge of detecting, investigating and combating cybercrime. Kader and Minnaar (2015) said due to modern societies improved reliance on borderless and decentralised data. Technologies and cyberspace have been recognised as an easy target for criminals. Encryption is no longer fool proof; e-commerce is unsafe, and the internet is no longer safely in the hands of accountable individuals. Control over cyberspace has become a free for all and nothing is hack proof with old cyber security. As a result, tracing cybercriminals have become a gradually difficult task for law enforcement agencies. Owing to the rate with which crimes are perpetrated in cyberspace as well as the difficulties presented by investigations of such multi- jurisdictional character, the task of the identification, successful investigation and prosecution of cybercriminals reflects rising challenges to law enforcement agencies across all boundaries both physical and in cyberspace.

Conventional investigative processes do not meet the demands of the tests associated with the investigation of cybercrime. Technical innovations have made it gradually difficult to answer the investigative questions of who, what, where, when and how. In this study, the researcher argued that the technical aspects and procedures of investigations into cybercrime are also still developing in response to the growth and changing of cyber-attack/hacking modus operandi of cybercriminals. Furthermore Basdeo (2012) explains that the expansion of search and seizure of electronic evidence powers are amongst the most controversial matters to confront the criminal justice system. Most of the significances of search and seizure of electronic evidence impact on and tests traditional laws governing criminal investigation and criminal justice. In addition, Jordaan (2019) points out that there is no doubt that cybercrime in its various forms is an important threat worldwide, with law enforcement worldwide struggling to war this insidious risk? It is a global crime delinquent with organised illegal clusters functioning across borders and becoming increasingly sophisticated as months go by. The South African Police Service (SAPS) aspects a continuous crime circumstances where the country is facing extreme levels of crime. However, the SAPS and the Directorate of Priority Crime Investigation

(DPCI) have recognised that cybercrime is a growing risk which has the probable to cripple the country.

## 2.5 HOW CAN INVESTIGATORS BE SKILLED ON CYBERCRIME?

Cross (2009:114) explains that it should be apparent that cybercrime detectives generally need broad training to work efficiently in this specialty area. This need is usually acknowledged in wide law enforcement agencies, where IT professionals and computer sciences might be enrolled to handle cybercrime investigations.

Categorising cyber investigators by skill set involves the following:

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

In addition, Edwards (2019:2) explains that due to the high capacity and complexity of cyber- attack should a victim opt to refer a complaint to police they cannot always count upon them to be available to tackle an investigation and locate the offender. Police resources are stretched and skilled cyber investigators in law enforcement are few and overworked. Irons and Ophoff (2016) explains that there are various large issues facing forensics investigators in South Africa. Cyber fear and cyber threat extent for South Africa and the problem in addressing the cybercrimes in the country through digital forensics are enormous. As a result, there is a need to develop strategy to check the threats through observation, for example, by analysing cybercrime reports. This will assist investigators to increase knowledge of modus operandi in cybercriminals. In this study, the researcher

argues for the development of digital skills among detectives or investigators in identification environment in KwaZulu- Natal Province in South Africa. Furthermore, such capacity may be applied in various similar settings in the country, but it must begin somewhere, and that is why the researcher sought to embark on finding solutions to cybercrime in the country. The study argues that there is a need to be advance digital expertise in South African through university programmes. According to Poonia, Banerjee and Banerjee (2016), crime changes with time and circumstances, meaning that it evolves. For this reason, criminals use sophisticated resources to ensure that they obtain their objectives, which is, making easy money. When one look at the sophisticated around all criminal activities, it is clear that criminals are very intelligent beings. They are able to use technology of high calibre which is often not easily available at the local market as they know that stakes are very high. The public should also begin to make it not easy for criminals to access private or personal information as this makes it easy for criminals.

The researcher was of the view that with the right skills and resources, as well as the adequate training, they can be able to make a difference by curbing cybercrime in South Africa. The researchers also emphasise that the police need extensive training to conduct crimes such as cybercrimes and other online crimes.

## 2.6 LEGISLATION THAT GUIDES CYBERCRIME IN SOUTH AFRICA

### 2.6.1 Act 25 of 2002 Electronic Communication and Transaction Act

In terms of section 85 of this Act, unless the context indicates otherwise" access" includes the actions of a person who after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.

### 2.6.2 Unauthorised access to interception of or interference with

According to section 86(1) is subjecting the interception and Monitoring Prohibition Act, 1992 (Act No 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission is guilty of an offense.

(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offense.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs adapt for use, distributes or possess any device, including a computer programme or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offense.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users are guilty of an offense.

### 2.6.3 Computer- related extortion, fraud and forgery

According to section 87(1), a person who execute or intimidate to perform any of the move described in section 86, for the purpose of getting any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to replace any damage caused as a result of actions, is guilty of an offense.

(2) A person who performs any of the move described in section 86 for the purpose of obtaining any illicit advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were original, is guilty of an offence.

### 2.6.4 Cybercrime Bill

The interesting developments was that in South Africa there is new Cybercrime Bill 2017 which was presented by the Portfolio Committee on Justice and Correctional Services, and the Bill was still to be signed by the Parliament Authorities at the time this research was conducted. The objective of this Bill is to create offences which have a bearing on cybercrime: to criminalise the distribution of data messages which are harmful and to provide for interim safeguard orders: to further control jurisdiction in respect of cybercrimes: to further regulate the powers to investigate cybercrimes: to further regulate aspects concerning to common assistance in respect of the investigation cybercrime: to provide for the establishment of a designed Point of Contact to further provide for the proof of certain facts by affidavit: to impose obligations to report cybercrime: 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. Reddy (2018) explains that the purpose of this is to determine the effectiveness of the Cybercrime Bill 2018 investigating and prosecuting cryptocurrency crime. The technique used to determine this enquiry is founded on the analysis of certain criminal, procedural and investigatory support necessities of the bill. An analysis of the Cybercrime Bill 2018 falls outside the scope of this research. The significance of this research rests on the increasing use of Cryptocurrencies in criminal activity (including money laundering, investment scams, fraud hacking and cyber extortion). The investigation and prosecution of such criminal activity may be exacerbated by the unique characteristics inherent in a cryptocurrency, a cryptocurrency is unregulated, online, encrypted currency denominated in its own units of value. Cryptocurrencies are thus an international online currency with multijurisdictional presence. Any criminal act related with its use will therefore invariably possess a cyber-element.

## 2.7 SUMMARY

This chapter presented the literature review on what other authors previously said about cybercrimes. It covers the research questions and the next chapter will be Research Methodology.

## CHAPTER THREE: RESEARCH METHODOLOGY

### 3.1 INTRODUCTION

The qualitative method was used in this study to collect the data and the researcher conducted interviews with Detectives of the South African Police Service (SAPS) at KwaZulu-Natal: Pietermaritzburg Clusters. The Police stations that were selected: Pietermaritzburg, Prestbury, Alexandra, Townhill and Pietermaritzburg DPCI Section. The researcher used purposive sampling in this study. The researcher is of the opinion that police detectives are the relevant population for this study, as they are dealing with different crimes including cybercrime on a daily basis. There were 16 participants (respondents) that were selected. In the following sections, the researcher discusses the research design, the target population and sampling, data collection, data analysis and the trustworthiness of the data, as well as ethical considerations.

### 3.2 RESEARCH DESIGN

The researcher adopted a qualitative approach while conducting this research as guided by Creswell 2009:173). Patton (2002) explains that qualitative researchers should strive to collect data in the field at the site where participants experience the issue or problem under study. Covid-19 did not make it possible for face-to-face interviews; however, the University provided guidelines to assist in data collection (See Annexure). As the Covid-19 Lockdown restriction relaxes, the researcher manages to conduct face to face interviews with participants This involves actually talking directly to participants and seeing them behave and act within their context or meeting them face-to face. This study utilised the ethnographic research paradigm as articulated in De Vos *et al*., (2011). The intent of ethnographic research is to obtain a holistic picture of the subject of study with emphasis on portraying the everyday experiences of individuals by observing and interviewing them and relevant others Gibbs (2007). The ethnographic study includes in-depth interviewing and continual and ongoing participant observation of a situation; and in attempting to capture the whole picture reveals how people describe and structure their world (Grasso and Epstein, 1992).

From 2019 to September 2020, I interviewed sixteen (16) participants using various methods due to challenges caused by Covid-19 pandemic. This was in line with Unisa's position on research which proposes alternative methods of conducting research. I believe that my experience as an investigator, as well as my understanding of the context

and my role, enhance my awareness, knowledge and sensitivity to many challenges under this study of cybercrime.

The researcher identified participants who would be in a better position to answer the research questions, as well as addressing the aim of this research. Having said this, it is significant to note that participants interviewed have vast experiences in the area of investigation in general and cybercrime in particular. De Vos *et al*., (2011:136) aptly point out that there are multiple-system designs which may be used while conducting research. In addition, Grinnell and Unrau (2008:166-178) suggests a fair number of possible designs of which the following five are of interest:

- The case study utilising a single-system design
- Experimental single-system designs
- Multiple designs for single systems
- Changing intensity designs and successive intervention designs
- Complex and combined designs

According to De Vos *et al*., (2011), the first step unique to the qualitative process is to select a paradigm and to consider the place of theory and a literature review in the research process. Furthermore, in selecting a paradigm, the first thing a researcher must outline is the paradigm that underpins the study – the researcher's point of view, or frame of reference in looking at life or understanding reality. Babbie (2007:31) defines a paradigm as the fundamental model or frame of reference we use to organise our observations and reasoning. In support of De Vos *et al*., (2011), Monette, Sullivan and DeJong (2008:37), posits that paradigms are fundamental orientations, perspectives or worldviews that are often not questioned or subject to empirical test. While a paradigm may not necessarily answer particular important questions, a paradigm may tell us where to look for answers.

Babbie (2007:32) alludes to the fact that all qualitative researchers approach their studies with a certain paradigm or worldview. Babbie (2007:33) further states that each of the paradigms offers a different way of looking at human social life. Each opens up new understandings, suggests different kinds of theory and inspires different kinds of research. For this reason, a researcher must choose a paradigm which is appropriate to the research being conducted and contextualise such paradigm to his/her research.

For the purpose of this study, the term design or designs is used for the equivalent of research design in the qualitative approach and will, therefore, refer to options available to qualitative researchers to study phenomena suitable for their specific research goal, referred to by some authors as strategies or traditions of inquiry.

## 3.3 EPISTEMOLOGY AND ONTOLOGY

Development and execution of research design depend on the way the researcher believes the research question(s) could be answered most truthfully and his/her assumption of how reality should be viewed by the researcher's ontology (Mason, 2002). The researcher in this study sought to answer the following questions:

- What was the impact of computer crimes in South Africa?

Readers will notice that the above question generated several sub-questions as highlighted on paragraph 1.5.1. of chapter one. Hofstee (2011:85) contends that research questions are sometimes used when not enough is not known about the problem to allow a thesis to be formulated or convincingly argued. For this reason, the researcher formulated research questions in an attempt to find out what exactly the problem with regard to cybercrime in South Africa is in general, and in selected areas in the Province of KwaZulu-Natal in particular. According to Flick (2007), the focus should be on the research question and the appropriateness of research design to clarify the research purpose and perspective. Mason (2002) argues that the first relevant question that the researcher should therefore ask when designing a qualitative study is: How should social reality be looked at? The next question that is therefore relevant for the research design is: What are the principles and rules by which I believe reality should be known? Or differently stated: What research perspective should I use to design my research? These questions by Mason assisted the researcher in formulating her questions in this study.

## 3.4 TYPES OF RESEARCH DESIGN

It is significant to note that there are various designs used by qualitative researchers. As a result, research designs depend on the purpose of the study, the nature of the research question and the skills as well as resources available to the researcher (De Vos *et al*., 2011:312). There are five qualitative designs available to the researcher, reflecting the most important schools of qualitative research (De Vos *et al*., 2011:307-323). These are ethnography, phenomenology, Grounded theory, Case study and narrative biography.

According to De Vos *et al*., (2011:308), qualitative researchers almost always develop their own designs as they go along, using one or more of the available strategies or tools as an aid or guideline. Denzin and Lincoln (2005) prefer to call methodologies such as ethnography, phenomenology and biographical methods "strategies of inquiry, or tools that can be used to design qualitative research". Similarly, Creswell (2007) identifies five traditional qualitative inquiries, which according to him, represent different disciplines, have detailed procedures and, most importantly, have proved to be popular and frequently used. These inquiries are the same as the ones highlighted by Denzin and Lincoln (2005), which are narrative research, phenomenology, grounded theory, ethnography and case study. Narrative-biographical designs refer to both product and process (Schwandt, 2007). Schwandt argues that this approach is based on the assumption that the life world of a person can best be understood from his/her own account and perspective. For this reason, the researcher in this study sought to understand the phenomenon based on participants' responses. These approaches are presented in the following section.

### 3.4.1 Narrative biography

Denzin and Lincoln (2005) believe that the researcher should gather and present data in such a way that "the subjects speak for themselves". In this research, the researcher sought to find the one that would comprehensively address both research questions as well as research aim/purpose. The purpose of this study is to analyse the impact of computer crimes in South Africa and determine whether South African Police detectives possess the relevant skills needed to investigate cybercrimes, computer crimes and online crimes.

Choosing a particular approach often negatively affects the quality of research because the combination of these qualitative research designs and inquiries would ensure rich and quality outcomes. According to Flick (2006), the main challenge of a narrative design is generating a question that will allow a narrative to develop that is not interrupted or obstructed by the interviewer. For this reason, narrative biography would not be appropriate for this research. The researcher had to explore other forms of research designs.

### 3.4.2 Grounded theory

Schram (2006) believes that the aim of this theory is to develop a substantive theory that is grounded in data. Moreover, grounded theory focuses on generating theory based on the study of social situations. The researcher did not choose this approach since her research did not involve theory development, but her study was aimed at finding real solutions for real challenges, that is, cybercrime.

### 3.4.3 Case study

Creswell (2007:184) describes a case study as a study which involves an exploration of a "bounded system" (bounded by time, context and/or place), or a single or multiple case, over a period of time through detailed, in-depth data collection involving multiple sources of information. The exploration and description of the case takes place through detailed, in-depth data collection methods, involving multiple sources of information that are rich in context. These may include interviews, documents, observations or archival records. Moreover, the researcher needs access to, and the confidence of participants. Babbie (2007) points out that case study researchers seek to enter the field with a knowledge of the relevant literature before conducting the field research. Case studies can be particularly useful for producing theory and new knowledge, which may inform policy development (De Vos *et al*., 2011:321).

The main approach reflects the belief that reality should be interpreted through the meaning that research participants give to their real-life world. The research designs of narrative biography, ethnography, phenomenology, grounded theory and case study are linked to each of the major perspectives as methodology (De Vos *et al*., (2011).

The researcher describes the term "research design" in accordance with the available literature on the concept. She then describes the intended design and approach to be followed during the research process. Welman *et al*., (2005) refer to the concept of a research design as the plan to find participants and how to collect information from them and analyse it. Mason (2002) states that the research design should not be seen as the only guide to the processes, since the methodology of qualitative research is fluid and flexible. De Vos *et al*., (2011) cite Babbie (2007) and refer to research design as a set of decisions with regard to the issue to be researched, the population group, the methods and the purpose of the research. De Vos *et al*., (2011) describe this part of the process as the decision, based on the suitability of the approach best suited to the intended

research, to choose between the quantitative, qualitative or mixed-method research approaches.

### 3.4.4 Ethnography

The researcher then looked at ethnography to determine if it could be appropriate for this research. Ethnography is characterised by using participant observation and an extended participation in the field, employing all sorts of methods (Flick, 2006). As a result of Covid-19 protocols and regulations, prolonged participation or observation would not be possible, bearing in mind the risks involved for both the researcher and participants. Ethnography is defined by (Creswell, 2007:242) as the study of an intact cultural or social group (or an individual or individuals within that group) based primarily on observations over a prolonged period of time spent by the researcher in the field. Rubin and Babbie (2010:391) state that a good ethnographic study will give one an intimate feel for the way of life observed by the ethnographer. However, Flick (2006:230) cautions that the interpretation of data and the questions of authority and authorship in the presentation of results must receive attention, as this approach may be perceived to be compromised. De Vos *et al*., (2011:315) posit that the aspirant researcher should be acutely aware of the fact that ethnographic fieldwork is not a straightforward, unproblematic procedure whereby the researcher enters the field, collects the data and leaves it unscathed. Research shows that the development of a global society necessitated changes in the method of ethnographic research to include virtual communities of cyberspace (Angrosino, 2007). This was perceived by the researcher to be appropriate as it is in line with Unisa's position on research approach due to Covid-19 pandemic.

### 3.4.5 Phenomenology

With regard to phenomenology, the aim was to describe what the life/lived world of participants consists of, as well as what concepts and structures of experience give form and meaning to it (Schram, 2006). Creswell (2007:57) regards a phenomenological study as a study that describes the meaning of the lived experiences of a phenomenon or concept for several individuals. This means that the researcher must strive to understand the phenomenon under study and be able to provide a description of human experience in that setting. According to Schram (2006), researchers must be able to distance themselves from their judgements and preconceptions about the nature and essence of experiences and events in the everyday world. Moreover, in this kind of setting, data are

presented in relatively raw form to demonstrate their authenticity. This is evident in the presentation of data in Chapter Four. This approach also requires the researcher to view social life in an unbiased, open-minded way and thus to “bracket” his/her own knowing of how encounters are socially structured or accomplished in order to describe the way members in a specific setting accomplish their own sense of structure (Schwandt, 2007). An example of a study utilising phenomenology is that of Groenewald (2003), who conducted research on cooperative education, which, based on his experience and literature review, he found to be often misunderstood or poorly practiced. Following this research strategy, his questions were directed at the meaning of participants’ experiences, feelings, beliefs and convictions about the theme in question. The researcher in this study is in the similar situation as Groenewald. In addition, the researcher in this study also set aside (bracketed) her own preconceptions in order to enter the participants’ life world and to make sure that she did not influence participants in any way.

From the above it was clear that placing a study within a particular research design may compromise the research in terms of richness and quality. Moreover, choosing a particular design before actual data collection may possibly result in frustration on the part of both the researcher and participants if not carefully considered. The researcher must choose a design which he/she believes and is confident that such design is fit for purpose. Researchers need to be clear about how and why a particular design, method and data source will assist in addressing research questions rather than assuming that a particular one will be emphatical enough to provide them with the information needed (De Vos, *et al*., 2011:323). The researcher was able to build relations with participants as well as gatekeepers in the sense that approvals to conduct this research were obtained (See Annexures). A gatekeeper is regarded by (De Vos, *et al*., 2011:325) as the individual with the formal or informal authority to provide approval for access to research groups, sites or participants.

## 3.5 TARGET POPULATION AND SAMPLING

The researcher uses and explains the terms “target population” and “sampling” in this section. Her intended target population was subsequently defined and the sample that would be employed to address the research topic is described.

### 3.5.1 Defining Population and Sampling

Welman *et al*., (2005) perceive the population as all the units of analysis about which the researcher wanted to draw a specific conclusion. Stake (1995) describe the target population as the unit of analysis. These authors further state that population could consist of individuals, groups, organisations or social artefacts. De Vos *et al*., (2011) describe sampling as the process of selecting cases to be observed and selected to be interviewed from the larger population of the intended study. Welman *et al*., *(*2005) distinguish between two forms of sampling, namely “probability” and “non-probability” sampling. Probability sampling enables the researcher to determine the probability that any member of the target population can be included in the sample. On the other hand, non-probability sampling does not provide for the specific inclusion of any member of the target population. De Vos *et al*., (2011) assert that sampling means that a small group of respondents could represent the view of the total population.

### 3.5.2 The Actual Population and the Possible Sample Group

The researcher selected specific investigators familiar to the phenomenon under this study. These were investigators working in a specialised operations environment as the target population. The reason for this selection of a target population is that cybercrime was a sophisticated crime requiring in-depth experience to be able to detect and investigate. Thus, ordinary police officers with no investigative experience would serve no purpose for this research. As a result, ordinary police officers did not participate in this research. The intended sampling approach was non-probability sampling, and the sampling technique was purposive sampling. For this reason, the researcher selects participants that possess most of the characteristics that are representative of the attributes that will best serve the study goal. The sample consisted of seasoned detectives as well as the aspiring ones working in the detective environment. In order to triangulate the findings, three focus groups were assembled, with sixteen participants in each focus group in identified areas in the Province of KwaZulu-Natal. The researcher subsequently conducted interviews with these selected officers. Due to Covid-19 pandemic, some of the participants were contacted using various alternative social media platforms and telephone interviews in order to enrich the research.

## 3.6 DATA COLLECTION

As indicated above, the researcher used various methods to interview participants due to Covid-19 pandemic. During interviewing open-ended questions were used and that allows

participants to provide valuable data. The researcher collected the data by means of field notes that were related to a specific interview schedule. The interview schedule was prepared in advance and was approved by the supervisor to ensure the relevance and quality. At times, audio recordings were made of the interviews (with the permission of participants). Field notes were also taken to be transcribed, coded and analysed later as guided by (De Vos *et al*., (2011). Interview questions were piloted prior to actual interview sessions and amendments were made as/when required. All these were conducted with the guidance and approval by the supervisor. Collected data were transcribed, analysed and themes developed as discussed in chapter four. The aim of developing themes was to answer both the research question(s) as well as addressing the objective/aim of this research.

## 3.7 DATA ANALYSIS

De Vos et al., describe the process of qualitative data analysis as a process often viewed differently by the respective authors on the subject. It is also stated that the process should not be seen as a rigid formula for analysing data, but rather a guideline that may be changed and adjusted throughout the process. The process of data analysis displays a spiralling movement rather than a linear line of processes. In this study, the researcher used the data analysis spiral as guided by (Leedy and Ormrod, 2010:153; Creswell, 2009:185).

## 3.8 TRUSTWORTHINESS OF DATA

The trustworthiness of data determines validity, reliability, weaknesses and/or strengths of qualitative research (Babbie (2007). Babbie further argues that the main strength of qualitative research lies in the depth of understanding that it creates. Moreover, the flexibility of the research approach is also seen as a strength, as it allows for changes while the research is being conducted. Leedy and Ormrod (2005) assert that the validity of the findings could be supported by strategies such as extensive time in the field, thick descriptions, feedback from others, and respondent validation. De Vos *et al*., (2011) refer to the trustworthiness or quality of qualitative research by reflecting on the view of two prominent qualitative researchers (Lincoln and Guba). Lincoln and Guba (1999) state that the trustworthiness of qualitative research is determined by four alternative constructs, namely credibility, transferability, dependability and conformability.

### 3.8.1 Credibility

The goal here is to demonstrate that the inquiry was conducted in such a manner as to ensure that the subject has been accurately identified and described (De Vos *et al.,* 2011:419). In this study, the researcher has used sufficient participants and sources to reach a reliable finding. Furthermore, the researcher made sure that boundaries for the research were set correctly in order to ensure the credibility and quality of the study. The researcher addressed credibility of the process through triangulation of sources in terms of literature and participants. Lincoln and Guba (1999) as cited in (De Vos *et al*., (2011:420) outline various strategies for increasing the credibility of qualitative research:

- Prolonged engagement and persistent observation in the field;
- Triangulation of different methods;
- Peer debriefing;
- Member checks, and
- Formalised qualitative methods such as grounded theory and analytic induction.

Lincoln and Guba (1999) propose the following four alternative constructs they believe reflect the assumptions of the qualitative paradigm, namely transferability, dependability, conformability and credibility.

### 3.8.2 Transferability

Transferability requires the researcher to ask whether the findings of the research can be transferred from a specific situation or case to another (De Vos *et al., 2011:420)*. These can be achieved only if the collected data are deep and rich in meaning, in order to understand the findings as a deeper perception by the participants. The researcher also performed a pilot study to confirm the transferability of the findings and the concept of triangulation of sources also applied. Data from different sources were used by the researcher to corroborate, elaborate and illuminate the research in question.

### 3.8.3 Dependability

In this regard, the researcher asks and answers the question whether the research process is logical, well documented and audited. Questions such as, “were all interviews recorded and linked correctly to field notes and transcripts” should be asked when the dependability of qualitative research is addressed. The view of researchers in the field of qualitative research is that the context of the original research can change as new information becomes available during the research process. The researcher audio

recorded all interviews with participants and kept field notes and transcripts of the interviews.

### 3.8.4 Conformability

De Vos *et al*., (2011:421), conformability captures the traditional concept of objectivity. Lincoln and Guba (1999) stress the need to ask whether the findings of the study could be confirmed by another. The researcher has extensive knowledge in the field of crime intelligence and has been involved in crime investigation for a long time. In order to maintain a neutral focus when executing the study, the researcher had to bracket all the experience she had gained outside of the research methodology, and also had to include this bracketing in the development of the interview schedules. All of this gave the researcher the advantage of understanding the field to be studied and strengthened the conformability of the findings.

## 3.9 ETHICAL CONSIDERATIONS

Parts of the process as well as the ethical considerations are the applications that had to be submitted to be able to conduct the research. Participants were requested to sign consent forms prior to the actual interviews. These participants were further assured that their participation would remain anonymous and could withdraw from participation at any given time when they no longer wished to participate.

The researcher was always guided by the Unisa Policy (2016) on Ethics for Research and committed to following these guidelines rigorously to ensure the integrity of both the University and the researcher. The Unisa (2016) Policy on Research Ethics contains four basic principles regarding any research that involves human participants. These are listed as autonomy; mainly speaking to the autonomy (free will to choose) rights and dignity of the selected participants. Moreover, the researcher adhered to the SAPS permission to conduct research which was granted before data collection and interviews with participants commenced. Participants were assured that no harm should come to any participant in this research project, and that the research would benefit the whole of a target group as well as the SAPS in general. De Vos *et al*., (2011) describe several ethical issues such as avoidance of harm, voluntary participation, informed consent, violation of privacy and anonymity as only a few ethical principles to consider during research. The researcher throughout requested written consent from participants and was sensitive during data collection to check the comfort levels of the participants on a regular basis.

It was important for the researcher to obtain gatekeeper permission. This is the body or organisation in which the researcher intended doing the planned research. In this regard, permission to conduct research approval was obtained from the SAPS (See Annexure). The importance of gatekeeper permission is to ensure that none of the organisation's privacy policies and other restricted information would be accessed without permission, since that could lead to compromising the study as a whole. A large organisation that is also a legal entity, such as the SAPS, is strictly regulated in terms of access to its information. If the researcher accessed information without the necessary permission, it would have serious legal repercussions. The Ethical Clearance Committee from the College of Law also issued an ethical clearance certificate (See Annexure).

## 3.10 SUMMARY

This chapter dealt with the aspects concerning data analysis, interpretation and presentation. It highlighted the process of coding and development of themes and categories to make sense of data as presented by participants in the research process. It also presented the testing of emergent understandings and explanations, interpretation and development of typologies. The chapter closes with assessing the soundness of qualitative data presented by participants. Aspects such as the research design, target population and sampling, data collection, data analysis and the trustworthiness of the data were discussed in detail. The importance of ethics and the dimensions of ethics in the study were also discussed. The purpose was to demonstrate transparency in the researcher's methodology, as well as to allow future researchers in the same field to employ similar methods to obtain similar type results. Any research project has to be approached with scientific preciseness as discussed in this chapter. In conclusion, it is important to state that researchers should take equally great care in how they go about analysing data and describing the steps as they do in the actual application of techniques and procedures (De Vos *et al*., 2011:422).

## CHAPTER FOUR: PRESENTATION OF FINDINGS

### 4.1 INTRODUCTION

In this chapter, the researcher presents and analyses data which emerged following intensive interviews with participants in selected Police Stations in KwaZulu-Natal: Pietermaritzburg. Data analysis is the process of bringing order, structure and meaning to the mass of collected data (De Vos, *et al*., 2011:397). Moreover, the researcher developed themes targeted at answering both researches aims, as well as research questions posed in chapter one. As one reads some of the participants which were quoted verbatim, a thread is drawn which links these responses to their experiences with the phenomenon of cybercrime and their lived experiences with regard to the concept of this study. This chapter focuses on the findings from collected data and discusses results with reference to objectives and research questions. Moreover, findings in this research affords readers an opportunity to make sense of the research findings as obtained from participants. In some instances, participants' responses are quoted verbatim. Participants' comments and experiences are corroborated with relevant literature where applicable. The interpretation of this data is aimed at addressing the following objectives:

- To analyse the impact of computer crimes in South Africa,
- To determine whether South African Police detectives possess the relevant skills needed to investigate cybercrimes.

In this study, the researcher adopted a qualitative approach to achieve the above-mentioned objectives, and also to answer research questions. Due to Covid-19 pandemic, the researcher used alternative data collection methods in line with Unisa's position on research where it was not possible to meet participants face-to-face (See Annexure).

Covid-19 changed the way this research was conducted in that adjustments had to be made to collect data. The University of South Africa position on research document (Annexure), provided guidance with regard to various options such as telephone interviews, and other platforms. As lockdown levels were eased, face-to-face interviews were possible, however, certain protocols had to be maintained, such as social distance, wearing of masks and hand sanitisation. Collected data were arranged thematically with the assistance of the supervisor in line with Grinnell and Unrau (2005), who posits that data should be arranged in accordance to their relatedness. So, emergent themes were

arranged as presented in the following sections, and where necessary, participant's statements were presented verbatim.

Flick (2006) mentions that although interpretation is at the core of qualitative data analysis, its importance is seen differently in the various approaches or strategies. According to Kreuger and Neuman (2006:161), the researcher should " … *interprets data by finding out how people being studied see the world, how they define the situation, or what it means for them*". For this reason, in study, the researcher interpreted data by giving them meaning or making them understandable with the point of view of the people being studied (De Vos *et al*., 2011:417). The following section presents themes which emerged from participants' responses.

## 4.2 EMERGING THEMES

The purpose of developing themes involves the process of transforming data into findings which can be interpreted. In addition, this involves reducing the volume of raw information, separating significance from trivia, identifying significant patterns and constructing a framework for communicating the essence of what the data reveal (Patton, 2002). Broadly conceived, this is the activity of making sense of interpreting these data (Schwandt, 2007:6).

The researcher sought to allow participants to express themselves when answering questions using interview questions. As a result, participants' responses are largely quoted verbatim throughout this chapter. This is in line with the suggestions of Angrosino (2007) who supports an approach where "the subjects speak for themselves". In this study, it was important to use the words and phrases by participants themselves in order to enrich this research. In order to analyse data, the researcher used a data analysis spiral as guided by (Creswell, 2009:185; Leedy and Ormrod, 2010:153). Before analysis, the researcher coded raw data by hand with the assistance of the supervisor. According to Grinnell and Unrau (2005), the primary task of coding is to identify and label relevant categories or topics of data.

Bogdan & Biklen (2007:173), regards categorisation and coding as two distinct steps. On the contrary, (Flick, 2006; Kreuger & Neuman, 2006; Grinnell & Unrau, 2005) regard these as simultaneous activities. The idea behind coding was to reduce the data into small, manageable sets of themes and to write into the final narrative (De Vos, *et al*., 2011:410).

The researcher sought to explore insights and to understand experiences and meaning of cybercrime in the South African context. Furthermore, the researcher embarked on this study in order to understand a conceptual understanding of the cybercrime phenomenon, as well as to find solutions to cybercrime which affects different people and organisations in various ways. Furthermore, the researcher's interpretations and findings had to be grounded in the participants' social reality in order to present a valid reflection of the cybercrime phenomenon (De Vos, *et al*., 2011:414).

Throughout her research, the researcher used participants' responses to generate and analyse data as well as developing themes as presented below. The first step in her analysis involved the generation of themes from interview transcriptions in accordance with the advice of (Strauss & Corbin, 1990). The researcher captured ideas and thoughts to assist her in making sense of the data and the categories she had drafted right after analysing the first interview (De Vos, *et al*., 2011:414). As is evident from the presentation below, the objective was to generate as many themes as possible. In doing so, some irrelevant information was not used as doing so would not necessarily enhance the quality of the research. Theoretical saturation was reached when no new themes/categories emerged. A decision to discard or ignore immaterial data was taken when saturation was reached. The following section presents conceptual themes which the researcher believes provides a comprehensive perspective of participants in this research.

### 4.2.1 Theme 1: The modus operandi found in cybercrime

The literature presented in the previous chapter highlights the challenges caused by cybercrime in South Africa in general, and in KwaZulu-Natal in particular. Research shows that cybercrime poses a great risk to both private individuals, small or large corporations and organisations, not only in the country, but the whole world. While various organisations may have some kind of estimates in terms of losses, it is not always easy to calculate losses.

Van Puyvelde and Brantly (2019) argues that, in the last decade, the proliferation of billions of new Internet-enabled devices and users has significantly expanded concerns about cyber security. The question is: Is such security real, exaggerated or just poorly understood? The researcher sought to explore risks caused by activities and interactions of individuals and organised groups in cyberspace. From the participants' responses, it was evident that the impact of cybercrime in South Africa is a cause for concern. However,

the extent of these concerns can only be quantified based on reported or detected cases. These cybercrime challenges are often a result of highly sophisticated and well-resourced organised syndicates who are determined not to be tracked. Modus Operandi (MO) was defined by one participant as:

> "…*Cybercrime was a crime committed in various ways, as the technology evolves. They adapt to what the trend in the world, for example currently crypto currency, is prevalent with people wanting to trade in this currency as it is regulated by the South African Government. It looks like a lucrative investment to make. Cybercriminals will take advantage of this and will offer returns on a weekly basis for investments made with them. These investments are paid to the suspects who in return do not pay any interest back to investors. Emails interception is being seen where the cybercriminals hacks email servers and intercepts emails with account information therein"* (**Participant 1)**.
>
> "…*Criminals use all kinds of ways to use the internet to defraud and mislead people to purchase or invest money. For example, they would create a website starting that they supply engine parts. The public will phone or email the criminals. They will request a deposit, after paying the deposit they will forward documents with photos of the product that are being ordered, the victim will pay the full amount over and engine parts never get delivered. On enquiries the criminals will make all sorts of excuses* **(Participant 2).**
>
> *"…Positive fraudulent sites on Facebook, intercepting of emails and card scamming* (**Participant 3).**
>
> *"…The main objective of modus operandi is successful commission of crime concealing the identity of the culprit and effective escape plan from law in case of being caught. Technology is a double-edged sword which has bettered our way of living by effective means of communication but along with it has made us prone to new and effective means of fraud. There are various modus operandi usually adopted by the cybercriminals for the successful commissioning of their crime"* (**Participant 4)**.
>
> *"…Cybercrime was a technological crime and therefore criminals have to modify their tactics in order to seek the vulnerabilities in the system and process thereof.*

*The perpetrators use all of their resources to hide their identity. Cybercrime does not leave the physical traces as traditional crime and it's more often than not committed from remote locations"* (**Participant 5)**.

*"…Many people advertise property for sale online and in social media the scammers often ask for a deposit from the unsuspecting victim. Once the money is deposited into their account, they fail to honour the deal"* (**Participant 6)**.

*"…Due to fast evolving technology criminals use the following to target people: they will conveniently and anonymously on the internet unauthorised access to devices identity theft and online banking information theft, network infiltration. Culprit poses a seller of electronic gadgets and doesn't deliver them. The emails are infiltrated and sent as they are from known businesses, Adverts are used for phishing when there are false, false links that are sent to victims" (**Participant 7)**.*

*"…The same technique and methods are used by criminals to commit cybercrime. It doesn't differ, for example they will give the computer an instruction. Each hacker has his/her own method to commit crime"* (**Participant 8)**.

*"…Interception of email communications when monies are to be paid between companies with false banking details are provided, false websites are created by companies to receive false tenders. Sim-swops are done, online banking are initiated and business companies and government sites are infected by malware and ransoms are required"* **(Participant 9)**.

The above responses highlight different views about the question posed. It further shows that there were various modes of operation when it comes to cybercrime. As a result, there is a requirement for high impact training for investigators who are tasked in investigating such highly organised and sophisticated types of crime. In terms of the above responses, there is also a requirement for public awareness programmes which would assist in minimising cybercrime in general. Despite the different responses as highlighted above, these responses call on every person to remain vigilant and aware, as anyone may fall victim to cybercrime at any given time. Financial institutions may play a significant role in educating their clients to safeguard their personal details and ensure that steps are taken to protect their valuable assets. Research shows that, every day, people interact with hundreds, if not thousands, of unlike devices, each connected to the

Internet, forming a massive network of networks (Van Puyvelde and Brantly, 2019:1). For this reason, risks for one becoming a victim of cybercrime become more serious. The following theme presents responses about victims of cybercrime.

### 4.2.2 Theme 2: The victim of cybercrime

When asked their opinion about the kind/types of cybercrime victims, some participants had the following responses:

> *"…The victims of cybercrime are from all sectors, which include the wealthy, poor, self-employed and Government workers. Any person who believes that they can make money quickly falls victim. People who also fall for phishing scams, they will request to click on the link to update their passwords and account details. Persons who do not keep their computer updated with the latest antivirus or antispyware often fall prey to ransomware attacks* **(Participant 1)**.

> *"…Anyone can fall victim to cybercrime although it is obviously limited to those that are using the internet such as companies, organisations and individuals that fall prey to cybercrime criminals. These victims are more often than not unsuspecting of the threat and consequences of their actions"* **(Participant 2)**.

> *"…Agree on Businesses, elderly people and the general population of South Africa fall victim to cybercrime"* (**Participant 3 and 4)**.

> *"…Young people who are internet users, businesspeople whose emails are hacked, anyone who uses the internet can fall victim, Attorney secretaries receive the emails and respond to those emails believed to be from clients about changing of bank accounts and Government Departments"* **(Participant 5)**.

> *"…There were quite a number of cases about cybercrime affecting businesses and individuals. Companies are also affected by cybercrime such as documents stolen, personal data being utilised for fraud, scams, identity theft and ransomware being used to extort money. Victims of cybercrime are from all walks of life. This crime is not limited to the wealthy, poor, self- employed, businesses and Government departments* **(Participant 6)**.

> *"…Everyone, no exceptions"* **(Participant 7)**.

*"…People who are computer illiterate fall victim to cybercrime, corporate companies and individuals. The victims of cybercrime are walks of life"* **(Participant 8)**.

*"…Members of the community, attorney companies, bank account holders with large credit balances, government departments as well as municipalities"* ***(Participant 9)***.

It emerged that the majority of the participants were of the opinion that anyone can fall victim to cybercrime, regardless of age and status in society. For this reason, everyone has to be vigilant at all times.

### 4.2.3 Theme 3: The impact of cybercrime on South African community

When asked what the impact of cybercrime on the South African community, some of the participants said:

*"…Cybercrime has an enormous impact on the South African Community as they are not prepared for the various modus operandi that are used by cybercriminals. Citizens are too trusting when it comes to keeping their personal electronic information safe* "(**Participant 1)**.

*"…Due to the continuous upgrading, availability and affordability of smartphones, users often fall victim to cybercrime because more frequent use of the internet due to smartphones they is economic and financial impact on South Africa's economy, as a results of cybercrime there are financial losses by individuals"* **(Participant 2)**.

*"…The community really suffers from cybercrime because the banks are very strict on paying the clients out who have been compromised by this crime"* **(Participant 3)**.

*"…Deprive elderly of cash and there is loss of profit in companies"* **(Participant 4).**

*"…The public has become painfully aware of what cyber security experts have been warning about cybercrime e is on rise and that everyone is a potential target. Hackers have adopted gradually more in financial focus, as they request ransom (usually in crypto currencies such as Bitcoin) in exchange for revealing the affected*

*user's information. The strain of Petya/ NotPeyta affected thousands of South Africans"* **(Participant 5)**.

*"…Unsuspecting pensioners were scammed out of their pension pay-outs"* **(Participant 6)**.

*"…Internet fraud makes people lose a lot of money. Cybercrime has a direct impact on jobs, economic growth and investments. Some businesses have been forced to close down because they were negatively affected by the cybercrime"* (**Participant 7)**.

*"…There was loss of Revenues; card is being cloned by cyber criminals"* (**Participant 8)**.

*"…Fraud and cybercrime are seen as crimes which cripple the economy in our country. Government departments, businesses and communities are losing billions due to fraud and cybercrime syndicate on annual basis"* **(Participant 9)**.

The above responses indicate that cybercrime was regarded as a serious challenge for citizens as unsuspecting individuals and organisations alike are constantly targeted to be swindled of hard-earned financial resources by organised and sophisticated syndicates.

### 4.2.4 Theme 4: The Legislation that guides cybercrime in South Africa

Participants were asked to explain their understanding about legislation that guide cybercrime in South Africa, and they answered in various ways. The majority of the participants agreed that prosecution of cybercrime in South Africa was regulated by the Electronic Communication and Transactional Act 25 of 2002 (ECTA) and Cybercrimes and Cyber security Related Matters (the Bill). They further stated that The Evidential Provision of the ECT Act: Chapter III of the ECT Act deals with Facilitating Electronic Transaction and chapter 11 to 20 deals especially with Legal Requirement of data messages. According to participants, the following regulations further guides aspects about cybercrime:

- The Council of Europe Convention on Cybercrime, to which South Africa is a signatory.
- The Copyright Act 98 of 1978.
- Films and Publications Act 65 of 1996.

- The South African Police Services Act 68 of 1995.
- Regulation of Interception of Communications and Provision of Communications Related Information Act 70 of 2002.

### 4.2.5 Theme 5: Investigation of cybercrime in South Africa

When asked about cybercrime investigation in some participants said:

> *"…There was a shortage of SAPS officers who are conversant and have necessary skills to investigate these types of crime. The accessible resources are used to identify and locate the culprits, identify email header, bank accounts and contact numbers. The mutual legal assistance from other countries through Interpol if need arises. Currently all conventional methods are still being used in South Africa to investigate cybercrime. This includes Section 205 subpoenas to cell phone records and bank accounts. The IP addresses are found and investigated to try to establish where the cybercriminal had sent email"* (**Participant 1).**
>
> *"…Currently all conventional methods were still being used in South Africa to investigate cybercrime. This includes Section 205 subpoenas to cell phone records and bank accounts. The IP addresses are found and investigated to try to establish where the cybercriminal had sent email. Once the case is opened, the investigating officer will peruse the statements and decide what investigative measures should be taken to prove the case. The elements of fraud need to be proved and therefore when a computer was used, there is a need to trace the computer/ device used. The digital forensic lab will then mirror the device and find the evidence needed in a criminal court of law"* **(Participant 2)**.
>
> *"…South African Police find it's challenging to deal with online crime. This type of crime has no boundaries nationally and internationally compared to traditional crime. It makes it difficult for the police to detect such crime. The lack of resources as well as shortage of police officials adequately trained on cybercrime. Specialised unit (DPCI) there is a shortage of personnel to deal with the volume of cybercrime cases"* **(Participant 3)**.
>
> *"…The Investigation cases that involves computers often fail due to mistakes made at the preliminary stage of the investigation process where crucial digital evidence is being ignored, destroyed, compromised or inappropriately handled.*

*During investigation of cybercrime there needs to be minimal delays in responding to the crime. The delay also compromises the effectiveness of the investigation and makes the response inappropriate when it comes to deter the cybercriminals"* (**Participant 4).**

*"…The police have been hesitant to act promptly against cyber-attacks, as they panic for not having the adequate knowledge in responding to such crime scenes. The assumption is that an intrusion may be caused by the culprit unintentionally where the culprit may be looking around without the intent of compromising data often raised. Detection, understanding and reacting to the same attack for the company or individual affected can be much more complex as they don't know ahead of time, the method of access, the motive, the routes taken, the data stolen. That has to be pieced together from often sparse or incomplete records of network or system activities. Cyber-attack can be complex to diagnose when one need to know what has happened and under pressure from customers, managers, the press and regulators to figure it out. Like any investigation of a crime, there can be a lot of assumptions involved"* (**Participant 5).**

*"…Agrees that Section 205 are sent to banks for suspect profile or to trace the suspect"* **Participant 5 and 6)**.

*"…South African Police find it's challenging to deal with online crime. This type of crime has no boundaries nationally and internationally compared to traditional crime. It makes it difficult for the police to detect such crime. The lack of resources as well as shortage of police officials adequately trained on cybercrime. Specialised unit (DPCI) there is a shortage of personnel to deal with the volume of cybercrime cases.*

*"…Once the case was opened, the investigating officer will peruse the statements and decide what investigative measures should be taken to prove the case. The elements of fraud need to be proved and therefore when a computer was used, there is a need to trace the computer/ device used. The digital forensic lab will then mirror the device and find the evidence needed in a criminal court of law"* **Participant 7)**.

*"…There is a huge shortage of SAPS personnel who are knowledgeable and have required training to investigate such. The available resources are used to identify and locate the criminals, identify email header, bank accounts and contact numbers. The mutual legal assistance from other countries through Interpol if need arises. The docket opens, the electronic device is seized, and the electronic device is forwarded to the cybercrime lab for analysis. Device is sent to the clerk of the high court: the private attorney is appointed to conduct investigation because of Section 14 of Human Rights: right not to have communication infringed"* **(Participant 8)**.

*"…Cybercrime involves a paper chase through section 205 subpoenas to banking institutions; SABRIC plays a major role in this paper chase, investigation of the IP address. The docket opens, the electronic device is seized, and the electronic device is forwarded to the cybercrime lab for analysis. Device is sent to the clerk of the high court: the private attorney is appointed to conduct investigation because of Section 14 of Human Rights: right not to have communication infringed"* **(Participant 9)**.

### 4.2.6 Curbing cybercrime in South Africa

When asked about curbing cybercrime in South Africa, participants responded as follows:

"…*To conduct public awareness. It will be the most effective way to curb cybercrime in the South African community. The public must be warned of new trends and taught how to keep their personal information safe on the internet. Cybercriminals will always find the new ways of getting people to be a part of their money"* **(Participant 1)**.

"…*The bank uses OTP for internet use and warns customers on their websites on a regular basis. The SAPS do awareness campaigns and warnings are posted all over social media and advertising platforms"* **(Participant 2)**.

"…*Educate the citizens not to give out information, monitor bank accounts, they should not respond to unknown emails and to be more vigilant at ATM's"* **(Participant 3).**

"…*To make people more aware of the consequences of cybercrime"* **(Participant 4).**

"…*The cyber hub agree to, for people to report any cybercrime. All complaints are investigated, and the feedback received. Unfortunately cyber expertise are rare in South Africa. In order to improve the correct skills, there is a necessity for our government to finance resources. Business particularly the banks has been hit hardest by computer crimes. They have launched awareness campaigns and spent huge amounts of money on security. As a result, the criminals focus on the end user into situations where personal login details are compromised. The biggest effort to challenge the situation has been focused on phishing. "Phishing is a way of deceitful obtaining personal information such as password, ID numbers, credit cards details and money". The phishing emails request that the user verifies or updates their contact details or other sensitive information that directs the user to a fake website designed by the criminals. A major risk of phishing is that these websites can be imitation"* **(Participant 5).**

**"…***To conduct awareness to people to protect their personal information with a unique password on their gadget. Reduce to purchasing online" (***Participant 6).**

*"…The communities need to be sensitised on a continuous basis informing them of the potential risks, modus operandi used by cybercriminals as well as preventative measures that must be followed to avoid such crime or become the victim thereof. Mobile devices and computers must be secured with passwords, your identity and having effective systems in place to counter such attacks" (***Participant 7).**

"…*Constantly updating security software on systems, do not open unfamiliar sites, do not give any personal information to those sites and to take careful note of email addresses" (***Participant 8).**

"…Educate the community *through radio, pamphlets, newspapers and television, door to door cybercrime awareness and toll-free number so people can report such crime" (***Participant 9).**

### 4.2.7 Theme 6: SAPS cybercrime training versus other countries

When asked about training for cybercrime detectives some participants said the following:

"…*There were numerous platforms where training can be given to SAPS officials. It's up to the training division of the police to ensure that they are aware of these. Within DPCI (Hawks) training is given to police officers from other countries such as the United States, Israel and the United Kingdom. There is a huge need for training to be given to the detectives at station level. At the moment they rely on their conventional methods in investigating cybercrimes"* **(Participant 1)**.

"…*Don't think South Africa is on standard with training and the ECT Act is not sufficient to curb the crime. Saps does not have sufficient resources or personnel to handle the amount of crime reported"* **(Participant 2)**.

"…*Saps training was very poor"* **(Participant 3)**.

"…*There was a need for more courses in South Africa"* **(Participant 4)**.

"…*There was a huge need for training to be given to detectives at station level. At the moment they rely on their conventional methods in investigating crime"* **(Participant 5)**.

"…*SAPS do not train enough police officials on cybercrime and cybercriminals become more advanced in technology and SAPS officials are far behind. SAPS department trains officials on online short courses which impact negatively on fighting against cybercrime. The officials should be identified from initial training and selected officials should attend a full course of cyber training to keep up with cybercriminals"* (**Participant 6**).

"…*Although I have not personally received training with regards to cybercrime, SAPS have highly qualified individuals due to their internal and external training courses"* **(Participant 7)**.

"…*There was still a long way to go in terms of training, training is limited only to DPCI units. The training should be rolled out to general detective units"* (**Participant 8)**.

"…*Saps has the same level of training as for the rest of other countries" (***Participant 9)**.

### 4.2.8 The cybercrimes that the detectives encounter on daily basis

All participants point out the cybercrimes that they encounter daily. The following were mentioned:

- Ransomware attacks
- Cyber bullying
- Crimen injuria
- Email interception
- False webpages
- Data leakage
- Data spying
- Phishing
- Cryptocurrency
- Online fraud
- Cyber laundering
- Web page hacking
- Cyber espionage
- Malware attacks
- Obscenity and child pornography
- Online shopping fraud
- Online banking fraud
- Advance fee fraud
- Phishing
- Smishing
- Keyloggers
- Email interception
- Identity theft
- Card cloning
- Attorney/ client emails interception
- Sim swop of cell phone and account depleted

The qualitative method was used in this study to collect the data and the researcher conduct interviews with the South African Police Service (SAPS) Detectives at KwaZulu-Natal: Pietermaritzburg Clusters and DPCI Section. The police stations that were selected will not be mentioned due to the sensitivity of detective's work. Purposive sampling was used in this study. The researcher is of the opinion that police Detectives are the relevant population for this study, as they are dealing with different crimes including cybercrime on a daily basis. There were 16 participants that were selected for the study, but the researcher was only able to interview 9 participants due to their busy schedules. The participants were named respondent 1 to 9.

Figure 1 outlines the impact of cybercrime in South Africa. Figure 2 outlines participant's responses with regard to posed questions and the result of collected data during interviews. The responses by participants managed to answer all questions posed in chapter one as well as addressing the objectives / aim of this research. In this study, the researcher sought to address the following:

- **Question 1: Describe the modus operandi found in cybercrime**

  Upon interviewing the participants. The researcher established that all 9 participants agreed that there are different types of modus operandi they encounter on a daily basis.

- **Question 2: In your experience who falls victim to cybercrime?**

  All participants agree that everyone falls into the trap of cybercrime in South Africa: including individuals, communities, businesses and Government institutions.

- **Question 3: Describe the impact of cybercrime in South African community**

  All participants indicated that there was a huge impact of cybercrimes in the South African community, this involves scams of cell phone messages, unauthorised access to bank cards through the internet, card cyclones, cryptocurrency (Bitcoin) and fraud.

- **Question 4: The Legislation that guides cybercrime in South Africa**

  All participants agree that ECT Act 2002 Currently in South Africa the only legislation that relates to Cybercrime ECTA. The Act is not sufficient for several of cyber- attacks that have been seen in South Africa. The Cyber Bill is in the progression of being

reviewed in Parliament. Once the Bill is passed law enforcement will be better equipped to charge cyber criminals.

- **Question 5: How does police investigate cybercrime in South Africa?**

Participants agree that SAPS find it challenging to deal/ investigate online crimes as this crime has no boundaries compared to traditional crime. It makes it difficult to detect such crimes. There are shortages of SAPS personnel who are training to investigate online crime. Other participants agreed that they used Sec 205 sent banks for suspect profiles then a docket will be opened.

- **Question 6: How do we curb cybercrime in South Africa?**

The researcher established that all participants agreed that awareness of our communities will be an assistance in curbing cybercrimes such as education communities in rural areas, through radio stations, television, pamphlets and posters.

- **Question 7: Can you comment on SAPS cybercrime training versus other countries?**

Majority of participants agree that the SAPS needs continuous training in online crimes. Especially in police stations, those officials that are conducting cybercrime investigation are not properly trained compared to other countries. Three (3) participants disagree that SAPS training is the same level as other countries and DPCI officials are in possession of cybercrime skills and training.

- **Question 8: What are cybercrimes that the detectives encounter on a daily basis**

All participants agree that there are different types of cybercrime that they encounter daily.

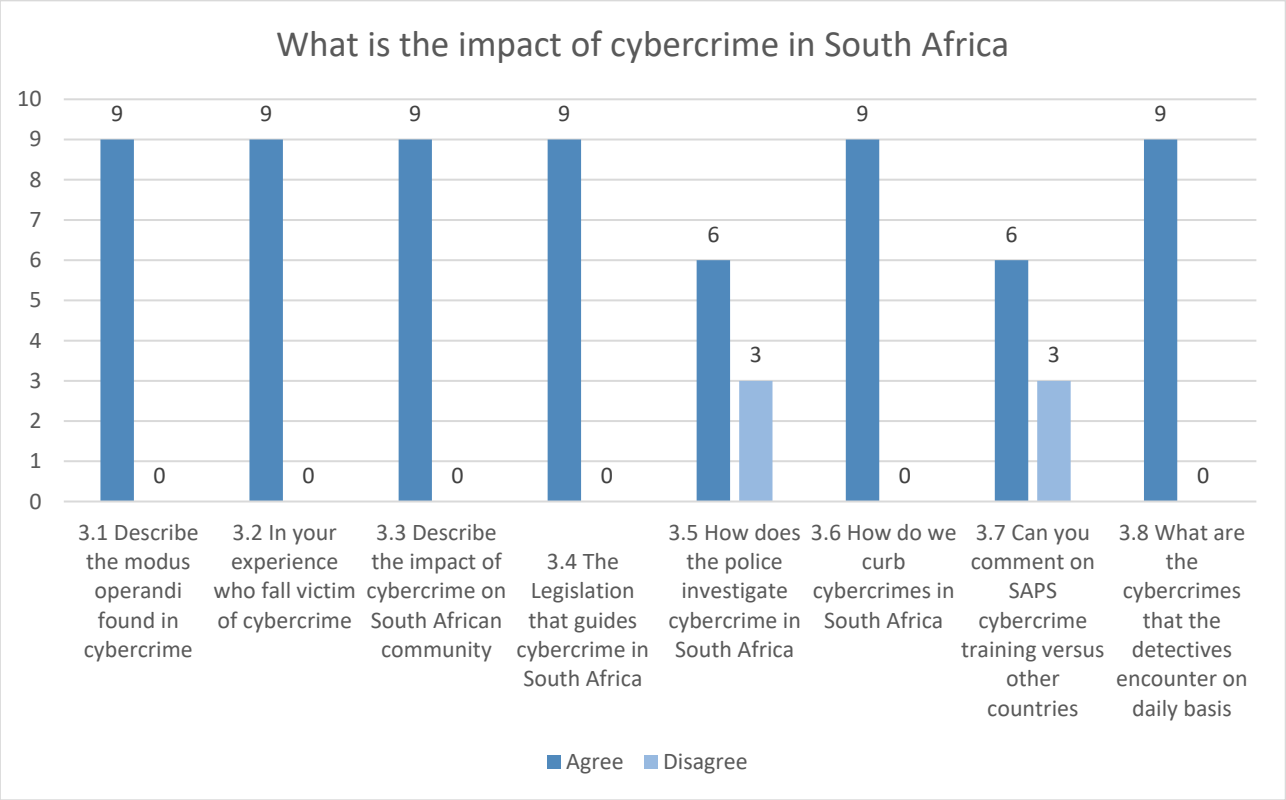



**Figure 1: Illustration of the analysis of the interviews**

It would appear that participants managed to address all questions regarding the challenges posed by cybercrime, an objective which the researcher sought to address in the beginning. It is also evident that, while not all issues would be addressed in this study, the researcher managed to find solutions with regard to pertinent issues which the general public may benefit from, in terms of vigilance and awareness. The researcher, therefore, proposes further research in this regard. Cyber security should be everyone's responsibility and not solely the responsibility of financial institutions and law enforcement agencies. Individuals and corporations can play a part to ensure that the risks associated with cybercrime is minimised or eradicated, thus making it difficult for syndicates and organised criminals to perpetrate crime.

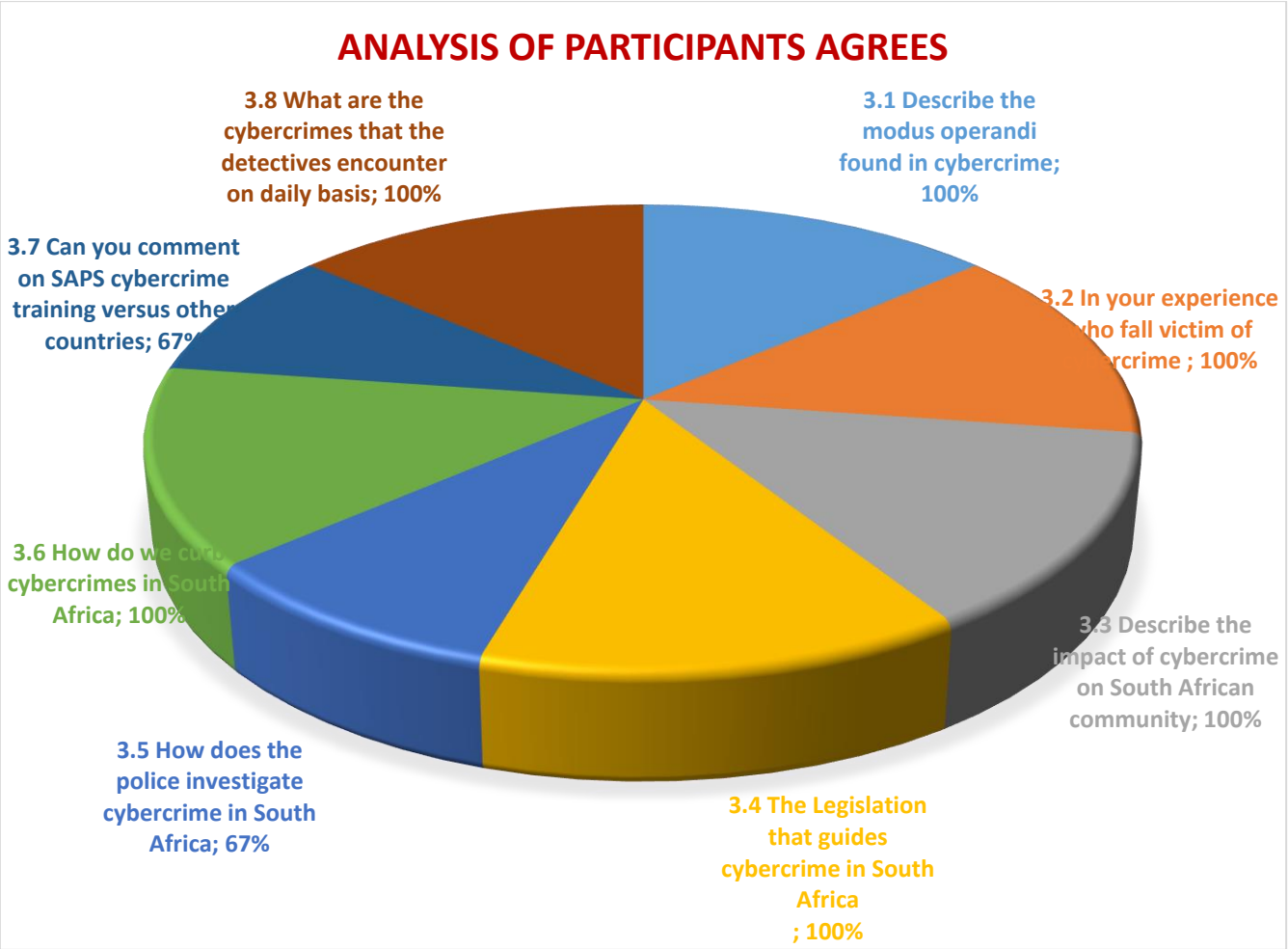



**Figure 2**

## 4.3 SUMMARY

This chapter analysed and understood the research findings. Interviews were conducted. The population that was selected were Detectives of the SAPS in KwaZulu-Natal; Pietermaritzburg and DPCI officials. Purposive sampling was used in this study. It was evident from the above that analysing, and interpreting data is no easy matter. Flick (2007:1-2) puts this as follows:

> *"In contrast to earlier stages in the development of qualitative research, questions about the quality of qualitative research are no longer raised mainly to demonstrate (from outside) that there is a lack of scientific quality in qualitative research. Rather this question is increasingly raised from the inside with a "how to" perspective: how to assess or evaluate what we are doing, how to demonstrate quality in qualitative research in an active and self-confident way".*

Chapter five recapitulates chapters from number one to four, and the related issues applied to reach conclusions. Recommendations will be completed in relation with the critical research findings, underlining the challenges of cybercrime as well as its impact on society in South Africa.

# CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

## 5.1 INTRODUCTION

This chapter concludes the research, focusing on the findings from collected data based on research questions as well as the research aim in chapter one and making recommendations. Findings in this research will hopefully guide authorities to design strategies to counter cybercrime in South African. As a reminder, the objectives of this research are the following:

- The research objectives were: To analyse the impact the cybercrime in South Africa
- To determine the procedures and techniques that were used when investigating cybercrime was still effective as cyber criminals are advances on daily basis

As highlighted earlier in this study, the researcher adopted a qualitative approach to achieve the above-mentioned objectives, and also to answer research subsequent questions. Due to Covid-19 pandemic, the researcher used alternative data collection methods in line with Unisa's Position on Research Ethics where it was not possible to meet participants face-to-face (See Annexure). However, there were instances where face-to-face interviews with participants were possible. These interviews were conducted following Covid-19 protocols. In this instance, all Covid-19 regulations such as social distancing, wearing of masks and sanitising were observed. Themes emanated from the collected data as outlined in the aforementioned chapter.

In the previous chapter, collected data were coded, themes developed, based on collected data, analysed and findings made. Based on these findings, recommendations are presented in the following section.

## 5.2 SUMMARY OF KEY FINDINGS

In this chapter, the researcher developed themes established on participants' responses. For this reason, findings in this section are centred on the following themes:

### 5.2.1 Theme 1: The modus operandi found in cybercrime

It emerged from participants' responses that there are various methods which perpetrators of cybercrime use, based on the ignorance or lack of awareness by potential victims. Moreover, it was found that, while financial institutions attempt to sensitise customers about the significance of personal protection of personal information by

customers, some remain unaware of the dangers of online transactions. Furthermore, it was found that criminals always develop new methods of tricking victims as they use sophisticated software and other high technical skills to bypass protective systems. It also emerged that organised cybercriminals operate from various parts in the world, making poorly trained detectives' work even more difficult.

### 5.2.2 Theme 2: The victim of cybercrime

It emerged that anyone can become a victim of cybercrime. However, those who are more aware are less likely to become victims. The concern remains of victims who are reluctant to report cybercrime, citing various reasons, ranging from fear of victimisation, lack of trust to law-enforcement agencies (apathy) and other reasons.

### 5.2.3 Theme 3: The impact of cybercrime on South African community

It was important to note that cybercrime can affect everyone in society, thus, it should be treated as a challenge of global concern. No person is immune to cybercrime. This means that all must remain vigilant and be aware of their transactions. Sometimes, cybercriminals do not want to attract attention, and for this reason, they may start with small amounts, and then graduate to bigger amounts gradually. It is also important for customers of financial institutions to ensure that they activate a system which reports every transaction, regardless of transaction.

### 5.2.4 Theme 4: The Legislation that guides cybercrime in South Africa

The researcher wanted to establish that there was legislation governing cybercrime in the country, and to ensure that there are no loopholes. It is prudent for South Africa to initiate Mutual Legal Agreement (MLA) with other countries. This will ensure that criminals can be pursued from remote countries where they operate from. Current legislation applies to criminals who operate from within the country. This finding is significant in the sense that cybercriminals have networks all over the world. So, if and when detected, authorities must be empowered to trace them without the challenge of legal boundaries (jurisdiction).

### 5.2.5 Theme 5: Investigation of cybercrime in South Africa

The issue of capacity and training was found to be a common challenge which requires urgent attention. It emerged that the majority of participants expressed concern about inadequate or lack of training related to cybercrime. It is particularly concerning that some

detectives deal with a huge number of cases, but do not possess the necessary skills to investigate such kinds of crime.

### 5.2.6 Curbing cybercrime in South Africa

It was not certain whether cybercrime can eventually be eradicated. However, pro-active measures can be taken to minimise its occurrence. Cybercriminals use sophisticated skills and resources; therefore, local detectives can only detect and solve cybercrime when they are well trained and resourced.

### 5.2.7 Theme 6: SAPS cybercrime training versus other countries

Specialised training in collaboration with law-enforcement agencies from around the world would ensure that detectives are empowered and well-resourced to deal with cybercrime. Investment in the form of training would be invaluable in ensuring safe spaces for all citizens.

### 5.2.8 The cybercrimes that the detectives encounter on daily basis

In chapter four (paragraph 4.2.8), the researcher highlighted some of the common cybercrimes that detectives encounter on a daily basis. From such a list, it is evident that detectives are overwhelmed, and may not be necessarily trained to deal with some of these crimes. Therefore, there is a requirement for all detectives to be properly trained and resourced. Based on the above, the following recommendations are made:

## 5.3 RECOMMENDATIONS

- Combating cybercrime does not rely only on technical skills only. An acute awareness of the ceaseless nature of cybercrime will be advantageous to Government departments, businesses and in society at large.
- As highlighted by participants, currently in South Africa the only legislation that guides cybercrime is Act 25 of 2002 ECTA. This Act is inadequate for dealing with several cyber-attacks that have been seen in South Africa. Fortunately, there is a new Cyber Bill which is in the process of being reviewed in Parliament. Once the Bill is passed, efficient prosecution of cybercriminals will be possible.
- It was recommended that SAPS should consider cybercrime procedures from other countries as cybercrime has no boundaries. Some cybercrime is committed in South Africa, whilst others are committed elsewhere in the world.

- Updating the training guides and procedures on a regular basis is necessary; to make sure that their relevancy as cybercrimes change constantly and cybercriminals are highly skilled.
- Recruitment of cybercrime investigators as there is an enormous shortage of personnel to investigate online crimes.
- There was a vast disparity between police investigators at the police station level and investigators in the DPCI Unit in terms of cybercrime training. It is recommended that the SAPS close the gap by cascading training in all police investigators.

## 5.4 THE SUGGESTIONS FOR FURTHER RESEARCH

The use of awareness campaigns appears to be effective to some extent. Therefore, continued efforts should be made in order to arrest the occurrence of cybercrime, not only in South Africa, but global. Moreover, it is also significant that communities remain vigilant and not become easy prey for cybercriminals. Additionally, authorities should consider signing mutual legal assistance with various countries to ensure effective and efficient investigation and prosecution of cybercrime. There is also a need to empirically assess global trends regarding cybercrime. Future studies in other provinces also need to be considered. This should include a wider range of participants, as the researcher has only involved participants in the area of this study, and no other parts of South Africa. Finally, an arrangement of in cooperation qualitative and quantitative research approaches also needs to be considered, as this type of research can be beneficial in defining optimal research questions and hypotheses identifying topical issues. Finally, the researcher is of the opinion that there is a need for further research in the following areas:

The research on online advertisements that are not authentic, where perpetrators advertise items that are for sale on certain sites and request the deposit and the balance of money, but they do not honour the promise.

The research on criminal conduct of cybercriminals as the technology changes on a daily basis.

## 5.5 CONCLUSION

Cybercrime has become a major threat and it is increasing drastically in South Africa. Cybercrime has no boundaries. Millions of Rands are lost through this crime. There are

various challenges that were established in this study. There is an immense shortage of police investigators that are properly trained on cybercrime. There are not enough resources to investigate cybercrimes. The gravity of the situation should be realised, and the recommendations of this study be practically implemented, in order to improve the SAPS operations and cybercrime investigations. The aim of this study was to:

- To analyse the impact of computer crimes in South Africa;
- and determine whether South African Police detectives possess the relevant skills required to investigate cybercrimes.

Various themes emerged from data collected from participants, which eventually answered both the research questions and research objective of this study. It emerged from the findings that the majority of participants believe that cybercrime has a negative impact, not only on the victims, but on the economy in general. The presence of legislation in itself is not adequate, but other efforts should be made to curb this scourge. The combination of legislation, awareness, and enforcement are most likely to be effective to curb cybercrime.

The purpose of this study was to analyse the impact of computer crimes in South Africa and determine whether the South African Police detectives possess the relevant skills required to investigate cybercrimes, computer crimes and online crimes. Based on the literature, contributions from participants and other sources information, it is my view that the objective of this study have been realised. Furthermore, this study will undoubtedly empower investigators in particular and law enforcement agencies to develop strategies to combat cybercrime. Further research with regard to the impact of cybercrime is required.

## LIST OF REFERENCES


Alazab, M. & Broadhurst, R. 2017. *An analysis of the nature of spam as cybercrime*. Cyber- physical security, 251- 266.

Anderson, G. & Arsenault, N. 2002. *Fundamentals of educational research*. 2nd edition. London: Routledge Falmer Taylor & Francis Inc.

Anderson, G. & Arsenault, N. 2005. *Fundamentals of Educational research*. 2nd edition. London: Routledge Taylor and Francis group.

Angrosino, M. 2007. *Doing ethnographic and observational research.* London: SAGE.

Ann-Carey, M. & Asbury, J. 2012. *Focus group.* London: Routledge Taylor & Francis group.

Aveyard, H. 2014. *Doing a literature review in Health and Social Care: a practical guide*. 3rd edition. Berkshire: McGraw-Hill Education.

Babbie, E. 2007. *The practice of social research,* 11th ed. Belmont: Thomson Wadsworth.

Babbie, E. & Benaquisto, L. 2010. *Fundamental of Social research*. 2nd edition. Toronto: Nelson Education.

Barbour, R. 2007. *Doing focus groups*. London: Sage publication Ltd.

Basdeo, V. 2012. The legal challenges of search and seizure of electronic evidence ion South Africa criminal procedure a comparative analysis. *South African journal of criminal justice* 25 (2): 195- 212.

Bidgoli, H. 2004. *The internet encyclopaedia*. Volume 1. California: Editor in chief.

Blankenship, D.C. 2010. *Applied research and evaluation methods in recreation*. Champaign: Library of Congress.

Bless, C., Highson-Smith, C. & Kagee, A. 2006. *Fundamental of Social research methods: an African perspective.* 4th edition. Cape Town: Juta Company Ltd.

Bless, C., Highson-Smith, C. & Sithole, S. 2013. *Fundamentals of social research methods: an African perspective.* 5th edition. Cape Town: Juta Company Ltd.

Bogdan, R. & Biklen, S.K. 2007. *Qualitative research for education: an introduction to theory and methods,* 4th ed. Boston: Allyn & Bacon/Pearson Education Group.

Bougaardt, G. & Kyobe, M. 2011. Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa. *Proceedings of the 2nd international conference on information management and evaluation*: Toronto 62, 2011.

Brace, I. 2008. *Questionnaire design*. 2nd edition. London: Kogan Page

Brits, M.T. 2013*. Computer forensics and cybercrime an introduction*. 3rd edition. Columbus: Pearson.

Broadhurst, R. 2006. *Developments in the global law enforcement of cybercrime policing an international journal of police strategies and management* 29 (3), 408-433, 2006 (Accessed 09/12/2019)

Brodber, K.S, Dwarika, A., Ellis, W, James, W. & Lashley, M. 2015. *Communication studies for Cape*. 2nd edition. Oxford: British library cataloguing in publication data.

Bryman, A. 2016. *Social research methodology*. Oxford: Oxford university press.

Bryman, A., Bell, E., Hirschsohn, P., Dos Santos, A., Du Toit J., Masenge, A., Van Aardit, I. & Wagner, C. 2011. *Research Methodology business and management context.* Cape Town: Oxford University press.

Casey, E & Ferraro, M.M. 2004. *Handbook of computer crimes investigation*. New York: Elsevier Academic Press.

Cassim, F. 2011. *Addressing the growing spectre of cybercrime in Africa*. Jaipur: Sabinet.

Cauvery, R., Sudha Nayak, U.K., Girija, M. & Meenakshi. 2003. *Research Methodology*. New Delhi: S. Chad & company Ltd.

Chamber- Jones, C. & Hillman, H. 2014*. Financial crime and gambling in a virtual world a new frontier in cybercrime*. Cheltenham: Edward Elgar.

Chawki, M., Darwish. A., Khan, M.A. & Tyagi, S. 2015. *Cybercrime, digital forensics and Jurisdiction*. New York: Springer.

Chawki, M., Darwish, A., Khan, M.A & Tyagi, S. 2015*. Cybercrime digital forensic and jurisdiction*. Ghaziabad: Springer.

Cooper, D.R. & Schindler, P.S. 2011. *Business research methods*. 11th edition. Boston: McGraw-Hill International edition.

Cooper, D.R & Schindler, P.S. 2014. *Business research methods*. 12th edition. Boston: McGraw- Hill International edition.

Cottrell, R.R. & McKenzie, J.F. 2011. *Health promotion and Education research methods; Using the five-chapter Thesis/ Dissertation model.* 2nd edition. Sudbury: Jones and Bartlett Publishers.

Creswell, J.W. 2007. *Qualitative inquiry and research design: choosing among five approaches.* London: SAGE.

Creswell, J.W. 2009. *Research design qualitative quantitative and mixed approaches*. Los Angeles: SAGE.

Creswell, J.W. 2014. *Research design qualitative quantitative and mixed approaches*. Los Angeles: Sage.

Creswell, J.W & Creswell, J.D. 2017. *Research design qualitative quantitative and mixed methods approaches*. 5th edition: Sage publication Inc.

Cross, M. 2008. *Scene of the cybercrime.* 2nd edition. Burlington: Syngress publishing Inc.

Denzin, N.K. & Lincoln, Y.S. 2005. *The SAGE handbook of qualitative research.* Thousand Oaks, CA: SAGE.

DePoy, E. & Gitlin, L.N. 2013*. Introduction to research: understanding and applying multiple strategies.* 4th edition. St Louis: Elsevier.

DePoy, E. & Gitlin, L.N. 2016*. Introduction to research: understanding and applying multiple strategies.* 5th edition. St Louis: Elsevier.

De Vos, A.S. 2002. *Research at grass roots*. 2nd edition. Pretoria: Van Schaik.

Desai, A. 2018. *Cybercrime cyber surveillance in South Africa*. Acta Criminologica: South African journal of criminology 31 (3), 149- 160.

Dlamini, S. & Mbambo, C. 2013. *An exploratory study on mechanisms in place to combat hacking in South Africa a criminological perspective*. Volume 3. pp 146- 154. (Accessed 03/04/2020).

Dlamini, S. & Mbambo C. 2019. *Understanding policing of cybercrime in South Africa the phenomena challenges and effective responses.* Cogent Social Sciences 5 (1), 1675404, 2019 (Accessed 12/12/2019)

Eadie, W.F. 2009. *21st Century communication: A reference handbook*. Volume 1. Los Angeles: Sage.

Edgar, T.W. & Manz. D.O. 2017. *Research methods for cyber security*. Cambridge: Syngress.

Edwards, G. 2019. *Cybercrime investigators handbook*. New Jersey: John Wiley & sons Inc.

Ezeji, C.L., Olutola, A.A. & Bello, P.O. 2018. *Cyber-related crime in South Africa extent and perspectives of state's role-players*. Acta Criminologica Southern African journal of criminology: 31 (3) 93- 110.

Fin24.2016. Alleged SA Ponzi scheme MMM's global pyramid collapses. https://m.fin24.com/money/investments (accessed on 28/04/2020).

Flick, U. 2006. *An introduction to qualitative research,* 3rd ed. London: SAGE.

Franklin, C.J. 2006. *The investigator's guide to computer crime*. Springfield: Charles C Thomas publishers.

Gibbs, G.R. 2007. *Analyzing qualitative data.* (*The SAGE Qualitative Research Kit*). Thousand Oaks, CA: SAGE.

Gillespie, A.A. 2015. *Cybercrime key issue and database*. New York: Routledge Taylor and Francis.

Gilmore, S. A. 2014*. PULP guide finding legal information in South Africa*. Pretoria: Pretoria University Law Press.

Gokhale, g. 2020. Network analysis of dark web traffic through the geo location of South African IP address. *Smart cities performability cognition and security*; 201-219.

Grasso, A.J. & Epstein, I. 1992. *Research utilization in the social services.* New York: Haworth.

Grinnell, Jr, R.M. & Unrau, Y.A. 2005. *Social work research and evaluation: quantitative and qualitative approaches,* 7th ed. New York: Oxford University Press.

Grinnell, Jr, R.M. & Unrau, Y.A. 2008. *Social work research and evaluation: foundations of evidence-based practice*. New York: Oxford University Press.

Groenewald, T. 2003. *The contribution of operative education in the growing of talent.* Unpublished doctoral dissertation. Johannesburg: Rand Afrikaans University.

Gubrium, J.F., Holstein, J.A, Marvasti, A.B. & McKinney. 2012. *The SAGE handbook of interview research: the complexity of the craft*. 2nd edition. Sn: Sage.

Hakim, C. 2000. *Research design: successful designs for social and economic research.* London: Routledge.

Hart, C. 2002. *Doing a literature search: A comprehensive guide for the Social Sciences.* London Sage Publications.

Helfgott, J.B. 2008. *Criminal behaviour theories typologies and criminal justice*. Los Angeles: Sage.

Hennink, M. Hutter, I & Bailey, A. 2011. *Qualitative research method*. London: Sage publication Inc.

Hennink, M., Hutter, I. & Bailey A. 2011. *Qualitative research methods*. Los Angeles. Sage Publication

Hesse-Biber, S.N & Leavy, P. 2011. *The practice of qualitative research*. 2nd edition. California: Sage publication Inc.

Holloway, I & Wheeler, S. *Qualitative research in nursing and healthcare*. 3rd edition. Ames: Wiley Blackwell publication.

Hofstee, E. 2011. *Constructing a Good Dissertation: A Practical Guide to Finishing a Masters, MBA or PhD on Schedule.* Sandton, South Africa: EPE.

Irons, A. & Ophoff, J. 2016. *Aspects of digital forensics in South Africa interdisciplinary journal of information knowledge and management*: 11pp 273- 283

Jaishankar, K. & Ronel N. 2013. *Second international conference of the South Asian Society of criminology and Victimology*. Trinelvet: South Asian Society of Criminology and Victimology.

Jesson, J.K., Matheson, L. & Lacey, F.M. 2011. *Doing your literature review traditional and systematic technique*. Los Angeles: Sage.

Jordaan, J. 2019. The role of cybercrime investigation digital forensics. Servamus community-based safety and security: (10) 33- 37.

Kader, S. & Minnaar A. 2015. *Cybercrime investigations cyber- processes for detecting of cybercriminal activities cyber- intelligence and evidence gathering. Southern African* journal of criminology 2015 special edition 5: 67-81, 2015.

Kempen, A. 2019. *Fighting cybercrime requires an integrated and international effort the envisaged approach*. Servamus community-based safety and security magazine: 112 (1), 50- 54.

Kreuger, L.W. & Neuman, W.L. 2006. *Social work research methods: qualitative and quantitative applications.* Boston: Pearson Education.

Krishnaswamy, K.N., Sivakumar, A.I. & Mathirajan, M. 2006. *Management research methodology integration of principles methods and techniques*. New Delhi: Pearson education.

Kumar, C.R. 2008. *Research methodology*. New Delhi: APH publishing.

Kumar, A.P. 2009. *Cybercrimes law a view to social security publisher under the banner of YFI*. Anupa: Kumar.

Kumar, R. 2014. *Research methodology, a step by step guide for beginners*. Los Angeles: Sage.

Kumar, R. 2019. *Research methodology a step by step guide for beginners*. 5th edition. London: Sage publication.

Leedy, P.D. & Ormrod, J.E. 2005. *Practical research: planning and design. Ninth Edition.* New York: Pearson Merrill Prentice Hall.

Leedy, P.D. & Ormrod, J.E. 2010. *Practical research: planning and design.* New York: Pearson Merrill Prentice Hall.

Le Compte, M.D. & Schensul, J.J. 2010. *Designing & conducting ethnography research.* Toronto: Altamia.

Lehmann, D. 2006. *Evaluation measurement properties of college research*. Germany: Grin publication.

Lincoln, Y. & Guba, E. 1999. Establishing trustworthiness. In Bryman, A. & Burgess, R.G. (Eds), *Qualitative research Vol* III. London: SAGE.

Linda, V. 2013. *Salem press encyclopaedia of science.* [SI]: [sn].

Machi, L.A. & McEvoy, B.T. 2012. *The literature review six steps to success*. 2nd edition. California: Sage Publications.

Malapane, T.A. 2019. *A risk analysis of e-commerce a case of South African online shopping space.* 2019 systems and information engineering design symposium (SIED): 1-6

Mansell, R. & Hwaang, P. 2015. *The international encyclopaedia of digital communication and society*. Volume 2. Malden: Wiley Blackwell.

Mason, J. 2002. *Qualitative researching, 2nd* ed. Thousand Oaks, CA: SAGE.

Merriam, B.S. 2009. *Qualitative research a guide to design and implementation*. San Francisco: John Wiley & sons Inc.

Monette, D.R., Sullivan, T.J. & DeJong, C.R. 2008. *Applied social research: a tool for the human services,* 7th ed. Belmont, CA: Thomson Wadsworth.

Montesano, J.J. 2019. *The anti-forensic tactics techniques and procedures cybercriminals use to hide electronic evidence of crimes*. Utica College.

Moskowitz, S.L. 2017. *Cybercrime and business strategies for global corporate security.* Cambridge: an imprint of Elsevier.

Myers, M.D. 2009. *Qualitative research in business & management*. London: Sage publication.

Minnaar, A. 2016. Organised crime and the new more sophisticated criminals within the cybercriminals environment how organised are in the traditional sense. *Acta Criminologica Southern Africa journal of criminology*: 123-141.

Minnaar, A. 2019. *Cybercriminals cyber exertion online blackmailers and growth of ransom*. Acta Criminologica Africa journal of criminology and Victimology: 32 (2) 105.

Mishler, E.G. 2009. *Research Interviewing context and narrative*. London: Library congress Cataloging in publication data.

Nair, K.K., Dube, E. & Lefophane, S. 2017. *Modelling an IoT test bed in context with the vulnerability of South Africa*. 3rd IEEE international conference on computer and communication (ICCC): 244- 248.

Ncube, C. 2016. Journal of internet law. [SI]: [sn].

Ndara, V. 2013. *Computer seizure as technique in forensic investigation*. Unpublished Mtech Dissertation, University of South Africa: Pretoria.

Nel, W. & Burger, A. 2017. *Proving cybercriminals possession of stolen credit card details on compromised POS devices*. ICMLG 2017 5th international conference on management leadership and governance: 254.

Neuman, W.L. 2014. *Basics of Social research: qualitative and quantitative approaches*. 3rd edition. Harlow: Pearson Education.

Olu, O.J. 2020. Underground cyber economy and implication for Africa's development a theoretical overview. Global perspectives on victimisation analysis and prevention: 177- 189.

Patton, M.Q. 2002. *Qualitative research and evaluation methods,* 3rd ed. Thousand Oaks, CA: SAGE.

Parahoo, K. 2006. *Nursing research principles process and issues*. 2nd edition. New York: Palgrate Macmillan.

Poonia, A.S., Banerjee, C. & Banerjee, A. 2016. *Improvised cybercrime investigation model.* Proceedings of fifth International conference on soft computing for problem solving: 743- 751.

Quinian, C. 2011. *Business research methods*. North way: Cengage learning.

Reddy, E. & Minnaar. 2018. *Cryptocurrency a tool and target for cybercrime.* Acta Criminologica Southern African journal of criminology: (31) 71- 92.

Reddy, E. 2019. *Analysing the investigation and prosecution of cryptocurrency crime as provided for by the South African cybercrime Bill*. Statute law. Volume xx: 1-14.

Roddel, V. 2011. *The ultimate guide to internet safety*. 2nd edition. Florida: Library of Congress.

Ross, J.I. 2009. *Criminal investigations cybercrime*. New York: Infobase. Publishing.

Rubin, A. & Babbie, E. 2010. *Essential research methods for social work*. Belmont: Brooks Cengage learning.

Russell, A.L. 2014. *Cyber Blockades*. Washington: Georgetown university press.

Schutt, R.K. 2006. *Investigating the social world the process and practice of research*. 5th edition. Thousand oaks: Sage publication.

*SAPS crime annual report*. 2016/2017. www.saps.gov.za> 2016/ 2017 (Accessed on 18/02/2019).

Schell, B.H. & Martin. C. 2004. *Cybercrime a reference handbook*. California: Library of Congress Cataloging.

Schell, B. & Martin, C. 2006. *Webster's new world a hacker dictionary.* Indianapolis: Wiley publishing Inc.

Schram, T.H. 2006. *Conceptualizing and proposing qualitative research,* 2nd ed. Upper Saddle River, NJ: Pearson Education Inc.

Schmalleger, F. 2005. *Criminal Justice today*. 8th edition. New Jersey: Pearson education Inc.

Schwandt, T.A. 2007. *The dictionary of qualitative research,* 3rd ed. Thousand Oaks, CA: SAGE.

Seidman, I. 2006. *Interviewing as qualitative research: A guide for researchers in Education and the Social Sciences.* 3rd edition. New York: Teachers College press.

Serrao, A. 2017. *Millions of South Africans personal information may have been leaked online*. http://www.m.news24.html (Accessed on 17/10/2017).

Sicetsha, A 2018. SAPS cybercrime unit unable to function due to expired software licenses. http://www.thesouthafrican.com (Accessed on 17/09/2018).

Singh, M.M. & Bakar, A.A. 2019. A systemic cybercrime stakeholder's architectural model. *Procedia computer science*: 161 1147- 1155.

Sissing, S.K. 2013. A criminological exploring of cyber stalking in South Africa. Pretoria: UNISA.

Sirohi, M.N. 2015. *Transformational dimensions of cybercrime*. Delhi: Alpha editions.

Shandu, S.N, Maluleke, W. & Lekgau, K. 2019. The use of electronic filling for the commission of income tax fraud in South Africa an empirical study. *Acta criminological. African journal of criminology and victimology*; 32 (2) 167-192.

Smith, C. 2018. *Cybercrime now 55% of gross losses in South African banking industry*. http://www.m.news24.html (Accessed on 04/10/2018).

*South Africa has the third highest number of cybercrime victims worldwide*. 2018.

www.iol.co.za/mercury.html (Accessed on 21/06/2018).

South Africa. 2002. Electronic Communications and Transactions Act 25 of 2005. http://www.acts.co.za/electronic_act_2002/index.htm (Accessed on 11/12/2019).

Stake, R. 1995. *The art of case study research.* Thousand Oaks, CA: SAGE.

Stander, A., Dunnet, A. & Rizzo, J. 2009. *A survey of computer crime and security in South Africa.* Cape Town: University of Cape Town.

Steven, P. & Gilbert, K. 2013. *Investigating computer related crime.* 2nd edition. Boca Raton: CRC press.

Strauss, A.L. & Corbin, J. 1990. *Basics of qualitative research: grounded theory procedures and techniques.* Newbury Park: SAGE.

Tenenbaum, G. & Driscoll, M.P. 2005. *Method of research in sport sciences*. New York: British library cataloguing publication.

Turner, l. & Weickgenannt, A. 2009. *Accounting information systems control and processes*. Danvers: John Wiley & sons Inc.

Upagade, V. & Shende, A. 2010. *Research methodology*. New Delhi: S. Chand & Company PVT Ltd.

Van Niekerk, B. 2017. *An analysis of cyber incidents in South Africa*. African journal of information and communication: (20) 113-132.

Van der Waag- Cowling, N. & Leenen L. 2019. *Proceeding of the 14th international Conference on cyber warfare and security.* Western Cape: ACPI.

Van Puyvelde, D. & Brantly, A.F. 2019. *Cybersecurity: Politics, Governance and Conflict in Cyberspace.* Cambridge, UK: Polity Press.

Van Rooyen, H.J.N. 2008. *The practitioners guide to forensic in South Africa*. Pretoria: Henmar publication.

Van Wyk, B. [Sa]. *Research design and methods part 1.* [Sl][Sn].

Wallace, D.P. & Van Fleet, C. 2012. *Knowledge into action: research and evaluation in library and information science.* California: Library of Congress Cataloging in publication data.

Walliman, N. 2016. *Social research methods*. Los Angeles: Sage Publication.

Welman, C., Kruger, F. & Mitchell, B. 2005. *Research methodology*. 3rd edition. Cape Town: Oxford University Press South Africa.

Whitson, G. 2013. Salem press encyclopaedia. [SI]: [sn].

Zikmund, W.G., Babin, B.J., Carr, J.C. & Griffin, M. 2013. *Business research methods*. 9th edition. [SI]: Cengage learning

## ANNEXURE A: UNISA ETHICAL CLEARANCE


### UNISA 2020 ETHICS REVIEW COMMITTEE

ERC Reference No: ST147-2019

Name: WB Mngadi

**Date: 2020:06:29**

**Dear Windy Bawinile Mngadi**

**Decision: Ethics Approval from**

**2020:06:29 to 2023:06:29**

**Researcher:** Windy Bawinile Mngadi

**Supervisor**: Dr DQ Mabunda

*An analysis of cybercrime investigation by Directorate for Priority Crime Investigation*

**Qualification:** Master of Art in Criminal Justice

Thank you for the application for research ethics clearance by the Unisa 2020 Ethics Review Committee for the above-mentioned research. Ethics approval is granted for 3 years.

*The **Low risk application** was **reviewed** by the CLAW Ethics Review Committee on 29 June 2020 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.*

The proposed research may now commence with the provisions that:

**1. The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached.**

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee.

4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.

5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.

6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.

7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.

8. No field work activities may continue after the expiry date **2023:06:29**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

*Note:*

| | |
|---|---|
| *The reference number ST 147-2019 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.* | |

Yours sincerely,


Prof T Budhram
Chair of CLAW ERC
**E-mail: budhrt@unisa.ac.za**
**Tel: (012) 433-9462**

Prof M Basdeo
Executive Dean : CLAW
**E-mail: MBasdeo@unisa.ac.za**
**Tel: (012) 429-8603**

## ANNEXURE B: SAPS PERMISSION TO CONDUCT RESEARCH

**SUID-AFRIKAANSE POLISIEDIENS**  **SOUTH AFRICAN POLICE SERVICE**

**Privaatsak/Private Bag X 94**
**THE HEAD: RESEARCH**

Verwysing/Reference: 3/34/2

Navrae/Enquiries: Lt Col Joubert
AC Thenga

Telefoon/Telephone: (012) 393 3118

Email Address: JoubertG@saps.gov.za

**THE HEAD: RESEARCH SOUTH AFRICAN POLICE SERVICE**
**PRETORIA**
**0001**

**A. The National Head**
**DIRECTORATE FOR PRIORITY CRIME INVESTIGATION**

**B. The Provincial Commissioner**
**KWAZULU- NATAL**

**PERMISSION TO CONDUCT RESEARCH IN SAPS: AN ANALYSIS OF CYBERCRIME BY DIRECTORATE FOR PRIORITY CRIME INVESTIGATION: UNIVERSITY OF SOUTH AFRICA: MASTER'S DEGREE: RESEARCHER: WB MNGADI**

A-B.

1. The above subject matter refers.

2. The researcher, Ms WB Mngadi, is conducting a study: A critical analysis of the proficiency of cybercrime investigation by South African Police Service, with the aim *to analyse the impact of computer crimes in South Africa and determine whether SAPS detectives possess the relevant skills needed to investigate.*

3. The researcher is requesting permission to interview a total of sixteen (16) SAPS investigators in Kwazulu-Natal. At the Directorate for Priority Crime Investigation (DPCI) Commercial Unit, Pietermaritzburg, a total of five (5)

respondents (one (1) Captain and four (4) Warrant Officers will be interviewed. Detectives will also be interviewed at the following police stations: Pietermaritzburg (one (1) Warrant Officer and two (2) Sergeants), Town Hill (one (1) Warrant Officer and two (2) Sergeants), Alexandra (two (2) Warrant Officers and one (1) Sergeant) and Prestbury (two (2) Warrant Officers).

4. The proposal was perused according to National Instruction 1 of 2006. This office recommends that permission be granted for the research study, subject to the final approval and further arrangements by the offices of the National Head: Directorate for Priority Crime Investigation and the Provincial Commissioner: Kwazulu Natal.

5. We hereby request the final approval by your office if you concur with our recommendation. Your office is also at liberty to set terms and conditions to the researcher to ensure that compliance standards are adhered to during the research process and that research has impact to the organisation.

6. If approval is granted by your office, this office will obtain a signed undertaking from researcher prior to the commencement of the research which will include your terms and conditions if there are any and the following:

6.1. The research will be conducted at his/her exclusive cost.

6.2 The researcher will conduct the research without the disruption of the duties of members of the Service and where it is necessary for the research goals, research procedures or research instruments to disrupt the duties of a member, prior arrangements must be made with the commander of such member.

6.3 The researcher should bear in mind that participation in the interviews must be on a voluntary basis.

6.4 The information will at all times be treated as strictly confidential.

6.5 The researcher will provide an annotated copy of the research work to the Service.

6.6 The researcher will ensure that research report / publication complies with all conditions for the approval of research.

7. If approval is granted by your office, for smooth coordination of research process between your office and the researcher, the following information is kindly requested to be forwarded to our office:

- **Contact person:** Rank, Initials and Surname.
- **Contact details:** Office telephone number and email address.

8. A copy of the approval (if granted) and signed undertaking as per paragraph 6 supra to be provided to this office within 21 days after receipt of this letter.

9. Your cooperation will be highly appreciated

*South African Police Services* *Suid Afrikaanse Polisiedienste*


Privaatsak Pretoria Faks No. (012) 334 3518
Private Bag X94 0001 Fax No.

Your reference/U verwysing:

My reference/My verwysing: 3/34/2

Enquiries/Navrae: Lt Col Joubert
AC Thenga

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

Tel: Email:
(012) 393 3118
JoubertG@saps.gov.za


Ms. WB
Mngadi
**UNIVERSITY OF SOUTH AFRICA**

**RE: PERMISSION TO CONDUCT RESEARCH IN SAPS: AN ANALYSIS OF CYBERCRIME BY DIRECTORATE FOR PRIORITY CRIME INVESTIGATION: UNIVERSITY OF SOUTH AFRICA: MASTER'S DEGREE: RESEARCHER: WB MNGADI**

The above subject matter refers.
You are hereby granted approval for your research study on the above-mentioned topic in terms of National Instruction 1 of 2006.

Further arrangements regarding the research study may be made with the following office

The National Head: Directorate for Priority for Crime Investigation:

- **Contact Person:** Capt. S Potgieter
- **Contact Details:** 0825569310
- **Email Address**: potgietersunette@saps.gov.za

Kindly adhere to paragraph 6 of our attached letter signed on the **2019-11-26** with the same above reference number.

**MAJOR GENERAL**
**HEAD: RESEARCH**
**DR PR VUMA**
**DATE: 2020-08-27**

## ANNEXURE C: INTERVIEW SCHEDULE

**TOPIC: AN ANALYSIS OF CYBERCRIME BY DIRECTORATE FOR PRIORITY CRIME INVESTIGATION**

## RESEARCH AIM

The purpose of this study is to analyse the impact of computer crimes in South Africa and determine whether South African Police detectives possess the relevant skills needed to investigate.

## RESEARCH QUESTIONS

- What is the impact of cybercrime investigators in the South African Police Services?

The research sub-questions are as follows:

- What was cybercrime?
- What was the impact of cybercrime on the South African community?
- How does the police investigate cybercrime?
- What was modus operandi of cybercrimes?
- How can investigators be skilled on the cybercrimes?
- What was the legislation that guide cybercrimes in South Africa?

## SECTION "A"

## HISTORICAL INFORMATION

1. Which Section of the FS are you working for?
   ……

2. How long have you been working for this Section?
   ……

3. What academic qualification(s) do you have?
   ……

4. Did you undergo training regarding forensic analysis in your Section?
.....

5. Does your work include forensic report writing and/or case review?
……

## SECTION "B"

### THE STRUCTURE AND THE CONTENT OF THE FORENSIC REPORT

1. As a forensic analyst, why do you write a forensic report?
……
……
……
……
……
……
……

2. Is there a guideline (SOP) on forensic report writing at your work environment?
……
……
……
……
……

3. Does the current SOP address the requirements and the expectations of the intended client?
……
……
……
……
……
……

4. In your opinion, what is the most important information in the forensic report is required by the court?
……
……

……
……
……
……

5. What information do you think (or know) is not important in the content of the forensic report?

……
……
……
……
……
……
……

6. If you could make changes to the current SOP on report writing, what will such changes be?

……
……
……
……
……
……
……

7. What is the content of the forensic reports that you issue to the client?

……
……
……
……
……
……
……

## SECTION "C"

Title: **AN ANALYSIS OF CYBERCRIME BY DIRECTORATE FOR PRIORITY CRIME INVESTIGATION**

1. What do you think is the purpose of an SOP at your workplace?

……
……
……
……
……
……
……
……

2. Is the current SOP on report writing unique to your Section or it is also used by other Sections of the FS?

……
……
……
……
……
……
……

3. Are all the reports in your Section standardised, and what is the impact of such?

……
……
……
.....
.....
.....
.....
.....
.....
.....

4. What do you think hinders the standardisation of the forensic report in the FS?

……
……
……
……

……
……
……

5. What do you think should be done to achieve standardisation of the forensic reports in the FS?

……
……
……
……
……
……
……
……
……

**PARTICIPANT INFORMATION SHEET**

Ethics clearance reference number:
Research permission reference number:

2020-03-11

Title: **AN ANALYSIS OF CYBERCRIME BY DIRECTORATE FOR PRIORITY CRIME INVESTIGATION**

**Dear Prospective Participant**

My name is WB Mngadi and I am doing research with Dr DQ Mabunda a Senior lecturer in the Department of Police science towards a master's at the University of South Africa. We are inviting you to participate in a study entitled: A critical analysis of the proficiency of cybercrime investigation by South African Police Service (SAPS).

**WHAT IS THE PURPOSE OF THE STUDY?**

I am conducting this research:

- To analyse the impact the cybercrime in South Africa
- To determine the procedures and techniques that were used when investigating cybercrime was still effective as cyber criminals are advances on daily basis

**WHY AM I BEING INVITED TO PARTICIPATE?**

Sixteen (16) Detectives from Pietermaritzburg Police Stations and DPCI (HAWKS) contact details were given by the Captain from Pietermaritzburg DPCI.

**WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?**

To describe the role of participant in this research study.
The study involves the use of questionnaires.
Method of questions will be structured around the above topic:

- Cybercrime
- Investigation
- Evidence gathering
- Court processes
- Convictions
- Trial

The estimated duration of the interview is estimated to be around 2 hours – 2 hours 30 minutes.

**CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?**

Participation in this study is voluntary and you are not compelled and under no obligation to partake in this study. If during the process of the study, you feel that you cannot continue with the interview and want to withdraw, you are free to withdraw anytime, and no reason will be required for this withdrawal. If you decide to take part in this study, you will be given this information sheet to keep and will then be asked to sign the written consent.

**WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?**

By taking part in this study, the participant will benefit by gaining more knowledge about Cybercrime cases.

- ICT

- Corruption
- Procurement processes
- White-collar crime
- Hacking

**ARE THEIR ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?**

Nil to low level inconvenience to the participant is expected from the interviews. No foreseeable risk of harm or side-effects to the potential participants has been identified. There is no harm or injury that is associated or expected from the study or the environment of the study but in case of such occurrence, the participant will be withdrawn from the study.

**WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?**

You have the right to insist that your name not to be recorded anywhere and that no one, apart from the researcher, the supervisor and any identified members of the research team, will know about your involvement in this study. Your answers will be given a code number or a alias and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings.

Your answers may be reviewed by people responsible for making sure that research is done properly, including the transcriber, external coder and members of the Research Ethics Review Committee. Records that directly identify you will only be available to people working on the study unless you give permission for other people to see the records.

Your anonymous data may be used for other purposes such as a research report, journal articles and or conference proceedings. A report of the study may be submitted for publication, but individual participants will not be identifiable in such report.

**HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?**

Hard copies of your answers will be stored by the researcher for a period of five years in a locked cupboard/filing cabinet [where? Indicate the location] for future research or academic purposes; electronic information will be stored on a password protected computer. Future use of the stored

data will be subject to further Research Ethics Review and approval if applicable. Hard copies will be shredded and/or electronic copies will be permanently deleted from the hard drive of the computer through the use of a relevant software programme.

**WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?**

You will not receive any remuneration for participating in this study

**HAS THE STUDY RECEIVED ETHICS APPROVAL?**

This study has received written approval from the Research Ethics Review Committee of Unisa and the SAPS. A copy of the approval letter can be obtained from the researcher if you so wish.

**HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?**

If you would like to be informed of the final research findings, please contact WB Mngadi on 061…… or 076……. The findings are accessible for 5 years. Should you require any further information or want to contact the researcher about any aspect of this study, please contact WB Mngadi on 061……. or 076……. or email: wbmngadi@gmail.com.

Should you have concerns about the way in which the research has been conducted, you may contact Dr D.Q. Mabunda on 012 433 9467 or mabundq@unisa.ac.za. Contact the research ethics chairperson of Unisa. The research ethics chairperson can be contacted on 012 429 3111 or www.unisa.ac.za if you have any ethical concerns.

## CONSENT TO PARTICIPATE IN THIS STUDY

I, _____ confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.
I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.
I agree to the recording of the interview.
I have received a signed copy of the informed consent agreement.

Participant Name & Surname……

Participant Signature……Date……

Researcher's Name & Surname
Researcher's signature…….. Date……

Thank you for taking time to read this information sheet and for participating in this study.
Thank you
WB Mngadi

## ANNEXURE D: EDITOR'S LETTER

word. services

Cell 083 556 1336 roneldavis430@gmail.com

28 May 2021

**DECLARATION OF PROOFREADING AND LANGUAGE EDITING**

To whom it may concern

I herewith declare that I did the proofreading and editing on **Windy Bawinile Mngadi's** dissertation in partial fulfilment of the requirements for the degree

**Master of Arts**

in the subject of

**CRIMINAL JUSTICE**

**AN ANALYSIS OF CYBERCRIME INVESTIGATION BY DIRECTORATE FOR PRIORITY CRIME INVESTIGATION**

and that I made suggestions for corrections regarding language, grammar, style and syntax, which were communicated to the student.

Please feel free to contact me should any additional information be required.

Sincerely

Ronel Davis

BA (Hons) UP

## ANNEXURE E: TURN-IT-IN REPORT

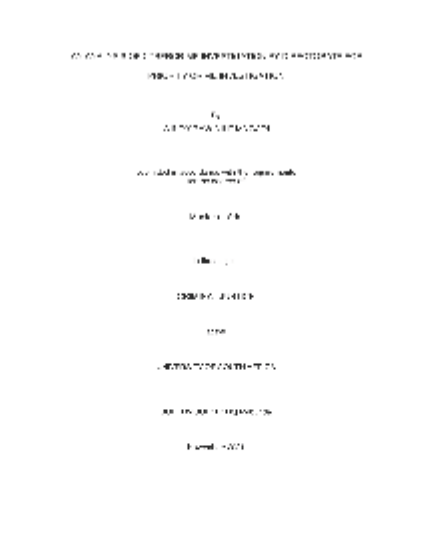
turnitin

# Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

| | |
|---|---|
| Submission author: | Wb Mngadi |
| Assignment title: | Revision 3 |
| Submission title: | An analysis of cybercrime investigation by Directorate for Pri... |
| File name: | MNGADI_DISSERTATION_2021_11_14_FINAL_VERSION_3.docx |
| File size: | 1.62M |
| Page count: | 105 |
| Word count: | 27,505 |
| Character count: | 157,446 |
| Submission date: | 14-Dec-2021 08:09PM (UTC+0200) |
| Submission ID: | 1730406102 |



## ANNEXURE F: UNISA COVID-19 POSITION STATEMENT ON RESEARCH ETHICS

*Prof T Meyiwa*
P. O. Box 392, UNISA, 0003
TELE: +27 (0) 12 429 2851
EMAIL: *meyiwt@unisa.ac.za*

**TO:** **ALL RESEACHERS**

**DATE:** 09 April 2020

**SUBJECT:** **UNIVERSITY OF SOUTH AFRICA COVID-19 POSITION STATEMENT ON RESEARCH ETHICS**

Dear Colleagues

On 15 March 2020 President Cyril Ramaphosa addressed the nation to declare a state of national disaster, following an increase in confirmed cases of COVID-19. The evolving COVID-19 pandemic requires that research is adapted on an ongoing basis to the dynamic situation.

A responsible approach to human participant, community engaged, animal, environmental, molecular and cell research is required in the context of COVID-19. Unisa supports the continuation of research activities, where possible, guided by the following principles and activities supported by the Policy on Research Ethics:

Protection of the participant, the community, and the researcher(s) and research support staff from any risks of harm while conducting research through the implementation of clear pragmatic risk mitigation measures.

Researchers must assess the risk - benefit ratio of a research study, particularly research that requires face-to-face contact, and the collection of data in public spaces or in locations where social distancing cannot be practiced.

The respect for the participant's rights for self-determination should always be carefully considered, for example the right to decline participation or to withdraw or collectively exploring alternative ways of participation.

In the interest of participants and researchers, the consensus is that new face-to-face or studies with an inherent risk to participants and/or researchers should not be embarked upon for the duration of the lockdown period.

Although this sounds like a blanket statement, registered Unisa Health Research Ethics Review Committees would be willing to consider well-motivated applications as exceptions only. The researcher needs to provide an accompanying letter with a detailed rationale for why this research study needs to be enacted during this time.

Unisa Ethics Review Committees (ERCs) will continue to accept and review research ethics applications but will clearly indicate where the ERC does NOT wish this study to commence with immediate effect in accordance with the lockdown regulations.

No research involving face-to-face contact or research studies involving settings where it is difficult to institute social distancing or practice protective measures may continue without formal notification and approval by the ERC that granted the approval in consultation with one of Unisa's registered Health ERCs/RECs.

Where or when it is unavoidable to reduce, suspend or postpone research activities, the onus is on the principal researcher to notify the ERC that approved the research study and to provide a rationale why the research needs to continue.

The ERC must inform the Unisa Research Ethics Review Committee (URERC) of all ongoing studies that may pose a risk of harm relating to the Covid-19 pandemic. National instituted protective measures such as hand hygiene, cough etiquette, and social distancing should be implemented, and monitored at sites where these studies will continue.

Research for degree purposes: The College of Graduate Studies and the Heads: Graduate Studies and Research will negotiate processes to mitigate the possible negative fallout to student progress (both new research and research that is in progress). The COVID-19 outbreak and its ramifications are difficult to measure or predict, but the suggested time frame for this position statement to be enacted is not less than the lockdown period.

Staff, researchers and supervisors are requested to carefully monitor any further internal communications for directives and guidance on this matter. Researchers who are dependent on internal, and more so external, sources of funding and sponsorship should consider the potential risks that COVID-19 and social distancing strategies will have on project milestones and audit reporting deadlines. Where possible, researchers should engage with the funder/sponsor regarding these timeframes.