

**AN EXPLORATION OF THE USE OF INTELLIGENCE-LED POLICING IN
COMBATING CYBERCRIMES IN SOUTH AFRICA**

by

PIETER MANTJIE MATSAUNG

submitted in accordance with the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in the subject

CRIMINAL JUSTICE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF. DT MASILOANE

2023

DEDICATION

This thesis is dedicated to my late grandmother, Nakedi Mojapelo, who encouraged me to further my studies. I appreciate all the support and encouragement you gave me to understand the value of education in my life. I wish you were here to witness this great achievement and may your precious soul continue to rest in peace. I call myself a blessed one for having had you in my life.

ACKNOWLEDGMENTS

I would like to thank the Almighty God for giving me the courage, wisdom and strength to complete this thesis even though I felt like giving up along the way.

I take this opportunity to express my sincere gratitude to the following people and their organisations for assisting me in so many ways to complete this study:

- I am grateful to my supervisor, Professor David Masiloane for his support, mentoring and guidance. His patience, knowledge, experience and dedication to the study made it possible for me to complete this study successfully.
- I am grateful to my uncle, Frankie Mojapelo, who supported and encouraged me to study hard.
- To my wife and daughter, Happy Mulalo and Nakedi Khano Matsaung, thanks for your love, support and understanding when I was always going to the library to study. Without your patience and support I would not be where I am today. Thank so much!
- To my parents, Paul Lesetja and Francinah Malekoba Matsaung who supported me throughout my education.
- To my siblings, Michael Tshidiso and Albert Kabelo Matsaung, for support and encouragement.
- The Department of Correctional Services that granted me study leave throughout the study.
- The South African Police Service and Directorate for Priority Crime Investigation that granted permission to interview their members.
- The members of the South African Police Service and Directorate for Priority Crime Investigation in the Limpopo, Gauteng, Mpumalanga, North West and Free State Provinces who participated in this study.
- Lastly, I would like to thank the University of South Africa for granting me a bursary for my studies from Master's Degree to Doctoral Degree.

SUMMARY

The study explores the use of Intelligence-Led Policing to combat cybercrime in South Africa through intensive literature and empirical research. Semi-structured interviews were conducted with members of the South African Police Service and members of the Directorate for Priority Crime Investigation in the Limpopo, Gauteng, Mpumalanga, Free State and North West provinces, to obtain their lived experiences on the use of Intelligence-Led Policing to combat cybercrime. The dynamics of cybercrime and its impact on the economy is dealt with, including the challenges in using Intelligence-Led Policing and specific factors that restrict the prevention, investigation and successful prosecution of cybercriminals.

Indicating the value of Intelligence-Led Policing in policing operations and how such value could be used in the fight against cybercrime should the identified challenges that affect the effective and efficient use of this policing approach be addressed. Specific recommendations are made on the conceptual implementation of Intelligence-Led Policing, and misconceptions on the use of Intelligence-Led Policing, the expiration of investigating licences of cybercrime investigators as well as the reluctance of some cybercrime victims to testify, in an attempt to protect the reputation of their companies.

KEY TERMS: Intelligence-Led Policing, cybercrime, phishing, malware, hacking.

ACRONYMS

ACSC	: Australian Cyber Security Centre
AFP	: Australia Federal Police
AU	: African Union
BJA	: Bureau of Justice Assistance
CART	: Computer Analysis and Response Team
CERT	: Computer Emergency Response Team
CI	: Crime Intelligence
CJS	: Criminal Justice System
CMA	: Computer Misuse Act
COE	: Council of Europe
CPA	: Crime Pattern Analysis
CSIR	: Council for Scientific and Industrial Research
CTA	: Crime Threat Analysis
DCS	: Department of Correctional Service
DIKI	: Data, Information, Knowledge and Intelligence
DPCI	: Directorate for Priority Crime Investigation
ECT	: Electronic Communications and Transactions Act
EU	: European Union
FBI	: Federal Bureau of Investigation
FT	: Forensic Tool
FTK	: Forensic Tool Kit
GIS	: Geographical Information System
GPS	: Global Positioning System
HMIC	: Her Majesty Inspectorate of Constabulary
ICT	: Information Communication Technology
IDS	: Intruder Detection System
ILP	: Intelligence Led Policing
INTERPOL	: International Criminal Police Organisation

IP	: Internet Protocol
ISP	: Internet Service Providers
ITU	: International Telecommunication Union
MISS	: Minimum Information Security Standard
NCPS	: National Crime Prevention Strategy
NCIS	: National Criminal Intelligence Service
NCSC	: National Cyber Security Centre
NIM	: National Intelligence Model
NPA	: National Prosecuting Authority
OAU	: Organisation of African Union
OSINT	: Open Source Intelligence
POCA	: Prevention of Organised Crime Act
POPIA	: Protection of Personal Information Act
RICA	: Regulation of Interception of Communication and Provision of Communication-Related Information Act
RSA	: Republic of South Africa
SA	: South Africa
SABRIC	: South African Banking Risk Information Centre
SAPS	: South African Police Service
SIGINT	: Signal Intelligence
UK	: United Kingdom
UN	: United Nation
UNISA	: University of South Africa
UNODC	: United Nations Office on Drugs and Crime
USA	: United State of America
WSIS	: World Summit on the Information Society
WTO	: World Trade Organisation

TABLE OF CONTENTS	PAGE
DECLARATION.....	ii
DEDICATION.....	iii
ACKNOWLEDGEMENT.....	iv
SUMMARY.....	v
ACRONYMS.....	vi

CHAPTER ONE: GENERAL ORIENTATION

1.1 INTRODUCTION.....	1
1.2 THE BACKGROUND OF THE STUDY.....	3
1.3 PROBLEM STATEMENT.....	9
1.4 RESEARCH AIM AND THE RESEARCH OBJECTIVES.....	18
1.5 RESEARCH QUESTION.....	19
1.6 THE SIGNIFICANCE OF THE STUDY.....	19
1.7 DEFINITION OF COCEPTS.....	21
1.7.1 Intelligence-Led Policing.....	21
1.7.2 Cybercrime.....	22
1.7.3 Phishing.....	22
1.7.4 Malware.....	22
1.7.5 Hacking.....	22
1.8 RESEARCH DEMARCATION.....	23
1.9 ORGANISATION OF THE THESIS.....	23
1.10 CONCLUSION.....	24

CHAPTER TWO: CYBERCRIME IN SOUTH AFRICA

2.1 INTRODUCTION.....	26
2.2 THE OVERVIEW OF CYBERCRIME.....	27
2.2.1 Cybercrime Categories.....	29
2.2.1.1 Hacking and the hackers.....	29
2.2.1.2 Types of hackers.....	30
2.2.1.3 Other types of cybercrime.....	31
2.2.1.4 Malware.....	34
2.2.1.5 Sub-categories of malware.....	35
2.3 CYBER SECURITY.....	37
2.4 ENCRYPTION.....	38

2.5 THE PREVALENCE OF CYBERCRIME	39
2.6 THE IMPACT OF CYBERCRIME IN POLICING	41
2.7 THE CHALLENGES OF COMBATING CYBERCRIME.....	42
2.8 THE PREVENTION OF CYBERCRIME	44
2.9 CONCLUSION	46

CHAPTER THREE: THE USE OF INTELLIGENCE-LED POLICING TO COMBAT CYBERCRIME IN SOUTH AFRICA

3.1 INTRODUCTION.....	47
3.2 THE VALUE OF CRIME INTELLIGENCE IN COMBATING CYBERCRIME	48
3.3 THE USE OF INTELLIGENCE TO COMBAT CYBERCRIMES.....	49
3.4 THE INTELLIGENCE-LED POLICING CONCEPT.....	51
3.5 THE EVOLUTION OF INTELLIGENCE-LED POLICING	52
3.6 THE CHALLENGES ON THE USE OF INTELLIGENCE-LED POLICING TO COMBAT CYBERCRIME	53
3.7 THE USE OF INTELLIGENCE-LED POLICING IN COMBATING CYBERCRIME	55
3.8 THE VALUE OF USING INTELLIGENCE-LED POLICING IN PREVENTING CYBERCRIME	57
3.9 THE USE OF INTELLIGENCE-LED POLICING AS CYBERCRIME REDUCTION, CRIME CONTROL AND DISRUPTION	59
3.9.1 The use of Intelligence-Led Policing to Deal with Cybercrime Reduction	59
3.9.2 The use of Intelligence-Led Policing to Deal with Cybercrime Control	60
3.9.3 The use of Intelligence-Led Policing to Deal with Disruption of Cybercrime ...	60
3.10 THE ANALYTICAL TECHNIQUES FOR INTELLIGENCE-LED POLICING TO COMBAT CYBERCRIME	61
3.10.1 The use of Crime Mapping and Spatial Analysis to Understand Cybercrime	61
3.10.2 The use of Structured Thinking to Understand Cybercrime	62
3.10.3 The use of Crime Scripts to Understand Cybercrime	63
3.10.4 The use of Hypothesis by Crime Analysts to Understand Cybercrime	64
3.11 TECHNOLOGY ASSOCIATED WITH INTELLIGENCE-LED POLICING TO COMBAT CYBERCRIME	65
3.12 CONCLUSION	67

CHAPTER FOUR: INTERNATIONAL PERSPECTIVE ON THE POLICING OF CYBERCRIME AND INTELLIGENCE-LED POLICING

4.1 INTRODUCTION.....	68
4.2 BEST PRACTICES FROM SELECTED COUNTRIES ON THE POLICING OF CYBERCRIME	69
4.2.1 The policing of cybercrime in United Kingdom	69
4.2.2 The policing of cybercrime in the United States of America	70
4.2.3 The policing of cybercrime in Australia	72
4.2.4 The policing of cybercrime in South Africa	73
4.3 INTERNATIONAL LEGAL FRAMEWORK ON THE POLICING OF CYBERCRIME	77
4.3.1 The Council of Europe Convention on Cybercrime	78
4.3.2 The United Nations Convention	79
4.3.3 African Union	80
4.3.4 The International Telecommunication Union	82
4.3.5 Group of Eight (G8).....	83
4.4 THE INTERNATIONAL CRIMINAL POLICE ORGANISATION.....	84
4.5 THE USE OF INTELLIGENCE-LED POLICING TO COMBAT CRIME IN DIFFERENT COUNTRIES	84
4.5.1 The use of Intelligence-Led Policing in the United Kingdom to combat crime	85
4.5.2 The use of Intelligence-Led Policing in the United States of America	87
4.5.3 The use of Intelligence-Led Policing in Australia	88
4.5.4 The use of Intelligence-Led Policing in South Africa	89
4.6 CONCLUSION	90

CHAPTER FIVE: THE USE OF CRIME ANALYSIS TO COMBAT CYBERCRIME

5.1 INTRODUCTION.....	92
5.2 THE PURPOSE OF CRIME ANALYSIS.....	93
5.3 TYPES OF CRIME ANALYSIS IN POLICING	94
5.3.1 Operational crime analysis	94
5.3.2 Administration crime analysis	95
5.3.3 Tactical crime analysis	95

5.3.4 Strategic crime analysis	96
5.3.5 Investigative crime analysis	96
5.3.6 Intelligence crime analysis	97
5.4 THE CRIME ANALYSIS PROCESS TO COMBAT CYBERCRIME.....	98
5.5 THE PROCESS OF INVESTIGATION OF CYBERCRIME	101
5.6 THE CHALLENGES IN THE INVESTIGATION OF CYBERCRIME	102
5.7 THE ROLE OF INTELLIGENCE-LED POLICING IN THE INVESTIGATION OF CYBERCRIME	103
5.8 THE ROLE OF CRIMINAL JUSTICE SYSTEM IN COMBATING CYBERCRIME	104
5.9 THE THEORIES OF PUNISHMENT	105
5.9.1 Retribution theory	105
5.9.2 Deterrence theory	106
5.9.3 Rehabilitation theory	107
5.10 CONCLUSION	108

CHAPTER SIX: RESEARCH METHODOLOGY

6.1 INTRODUCTION.....	109
6.2 RESEARCH METHODOLOGY	109
6.3 RESEARCH DESIGN.....	110
6.4 RESEARCH METHODS	111
6.4.1 Research Approach.....	112
6.4.2 Population and Sampling Methods	112
6.5 PILOT STUDY.....	114
6.6 DATA COLLECTION.....	114
6.6.1 Interviews	115
6.6.2 Literature Review	118
6.7 DATA ANALYSIS	119
6.8 VALIDITY AND RELIABILITY OF THE STUDY	119
6.9 METHODS TO ENSURE TRUSTWORTHINESS OF THE STUDY	120
6.9.1 Credibility	121

6.9.2 Dependability	121
6.9.3 Transferability	122
6.9.4 Conformability	122
6.10 ETHICAL CONSIDERATIONS.....	123
6.11 CHALLENGES ENCOUNTERED IN THE STUDY	125
6.12 CONCLUSION	125

CHAPTER SEVEN: PRESENTATION, DISCUSSION AND INTERPRETATION OF RESEARCH FINDINGS

7.1 INTRODUCTION.....	127
7.2 FINDINGS	127
7.2.1 The role of Intelligence-Led Policing in the investigation of cybercrime	129
7.2.2 Investigative skills required in the investigation of cybercrime	132
7.2.3 The use of Intelligence-Led Policing by the South African Police Service to combat cybercrime	135
7.2.4 Challenges encountered in using Intelligence-Led Policing to combat cybercrime	138
7.2.5 Addressing challenges encountered in using Intelligence-Led Policing to combat cybercrime	139
7.2.6 The challenges encountered in the investigation of cybercrime	141
7.2.7 The impact of the challenges encountered in the investigation of cybercrime.....	145
7.2.8 Addressing the challenges encountered in the investigation of cybercrime	145
7.2.9 The strategy of the South African Police Service in the investigation of cybercrime	147
7.2.10 The strategy of the Directorate for Priority Crime Investigation in the investigation of cybercrime	148
7.2.10.1 Cybercrime Strategy for the South African Police Service and the Directorate for Priority Crime Investigation	149
7.2.11 The value of using Intelligence-Led Policing in the investigation of cybercrime in South Africa	152
7.3 CONCLUSION	153

CHAPTER EIGHT: RECOMMENDATIONS AND CONCLUSION

8.1 INTRODUCTION.....	155
8.2 RECOMMENDATIONS	155
8.2.1 Conceptual Implementation of the Intelligence-Led Policing	156
8.2.2 Misconception on Intelligence-Led Policing	158
8.2.3 Lack of Resources, Training and Fear	158
8.2.4 Investigation Licences	159
8.2.5 Hidden Identities	160
8.2.6 Unwillingness to Testify	160
8.2.7 Cybercrime Strategy	161
8.3 CONCLUSION	161
REFERENCE LIST.....	163
ANNEXURE A: INTERVIEW SCHEDULE OF DETECTIVES	179
ANNEXURE B: INTERVIEW SCHEDULE OF CRIME INTELLIGENCE.....	181
ANNEXURE C: INTERVIEW SCHEDULE OF DIRECTORATE FOR PRIORITY CRIME INVESTIGATION	182
ANNEXURE D: ETHICAL CLEARANCE.....	184
ANNEXURE E: TURN-IT-IN CERTIFICATE.....	186
ANNEXURE F: EDITING CERTIFICATE	187
ANNEXURE G: PERMISSION FROM THE SOUTH AFRICAN POLICE SERVICE.....	188
ANNEXURE H: PERMISSION FROM THE DIRECTORATE FOR PRIORITY CRIME INVESTIGATION.....	193

CHAPTER ONE: GENERAL ORIENTATION

1.1 INTRODUCTION

The use of computers created expedient communication opportunities in society such as the instant sending and receiving of messages from one person to the other, as well as any other very useful applications. Unfortunately, however, criminals also seized this opportunity to commit cybercrime, thus causing high levels of computer crimes (Ezeji, 2014:1). According to Mothibi and Amali (2018:57), cybercrime occurs when a person or persons commit crime by means of a computer where the computer becomes the object of the crime. Cybercrime makes it easy for organised criminal networks to expand nationally, regionally and internationally. Ezeji and Olutola (2018: 168) state that the most cybercrimes experienced in South Africa are online fraud, information theft, credit card fraud, identity theft, hacking, spreading of viruses, ransomware, espionage and theft of intellectual property. The accessibility of tablets, cell-phones and computers to most people, including potential criminals and criminal syndicates could be a contributing factor to facilitate the easy access for criminals to target individuals on social network sites to get essential information for the commission of these crimes. Such criminals take advantage of the low risk of detection for these crimes and the fact that they can be committed anywhere in the world. Minnaar (2014: 127) supports this sentiment by stating that the increased use of information technology creates opportunities for cybercriminals to target cyberspace and perpetrate various illegal activities online.

According to Minnaar (2016: 123), cybercrime is a form of organised crime operating underground for hacking bank accounts, selling stolen information, spreading viruses and providing backup services for criminal group networks. Cybercriminals become more skilled and sophisticated in spreading malware to attack cyberspace for financial benefits. They develop different types of malware viruses such as malvertisement, iframe script injection and ransomware to attack vulnerable victims who do not safeguard/protect their personal information or who could not afford to update their cyber-security protection measures. Ezeji, Olutola and Bello (2018: 93), state that cybercriminals use different methods to attack, such as the Worms, Trojan and

Backdoor programmes to gain access on computer systems or networks that help them to commit e-commerce fraud, identity theft, online credit card fraud, cyberbullying and the theft of personal information. According to Cassim (2012: 181-182), some organised crime groups and cyber-terrorists use computer technology to attack/assault governments, businesses, banks and infrastructure. Moore (2015: iii) indicates that those crimes have a huge impact on disrupting and crippling the entire economy such as the railways, electricity grids, airlines, nuclear power stations and large irrigation dams that depend on computer systems for their operation.

In the fight against cybercrime the police should also use or intensify the use of Intelligence-Led Policing, which is a police business model that collects large volumes of data from various sources and process such data into serviceable information. This model includes profiling of criminals, mapping of crime spots and prediction of the crimes that might ensue as well as how criminal networks might act (Ezeji & Olutola, 2018: 169). The use of Intelligence-Led Policing could enable the police to prevent, combat or successfully investigate cybercrime because Intelligence-Led Policing has proven to be successful in dealing with crime and criminality (Bureau of Justice Assistance, 2008: iii). It enables the police to target organised criminal networks, identify crime hotspots, and to link crime series by working together with other stakeholders to reduce crime and disorder (Govender, 2012: 83).

The collection of crime data by crime intelligence is used to make informed decisions on crime reduction and crime prevention strategies (Budhram, 2016: 81). The police use Intelligence-Led Policing to capture trends for observing criminal behaviour, including cybercrime over a certain time period and to target offenders who are expected to commit future crimes (Zinn, 2011: 13). This crime prevention model helps to collect, vet and compare large volumes of crime data to obtain a clear picture on criminals, their associations and crime scenes that present higher concentrations of crime within communities (Matsaung, 2019: 62). It is basically used as a risk assessment approach for crime management to target criminals, collect crime data, link repeat offenders, map, trace and predict crime patterns (Mashiloane, 2014: 179).

This study focuses on an exploration of the use of Intelligence-Led Policing in combating cybercrimes in South Africa because not much is known on the use of Intelligence-Led Policing in dealing with cybercrimes in this country. According to Ezeji and Olutola (2018: 186), Intelligence-Led Policing is a new paradigm shift from reactive to proactive policing and can help in combating technologically enhanced crime in South Africa. Canaday (2017: 23) regards it (intelligence-led policing) as a business model that may direct law enforcement agencies in decision-making, identification of crime hot spots, prolific offenders and criminal groups. According to Matsaung (2019: 58), the advantage of using Intelligence-Led Policing is to understand behaviour of offenders during the commission of cybercrime so that they can identify links and crime patterns between offenders and crime scene locations with the purpose of identifying crime series. It can also help police in a long-term strategic planning by incorporating technology such as cameras and closed circuit television as preventative measures to combat cybercrime. Intelligence-Led Policing should become a crime prevention approach that supports the operations of police and partnership policing to achieve objectives of policing through prevention, detection and investigation of organised crime, cyber terrorism and cybercrimes more effectively (Buckley, 2014: 32-33).

1.2 THE BACKGROUND OF THE STUDY

Cybercrimes are borderless crimes that pose jurisdictional challenges in a country as they can be perpetrated by a person or syndicates from anywhere in the world. The problem encountered by the criminal justice system is that only few officials have experience and the requisite training in the prevention, evidence gathering, investigation and prosecution of cyber offences (Ezeji et al., 2018: 95). A study conducted by the Federal Bureau of Investigation of the United States of America on cybercrime, places South Africa on number seven in the list of the countries that have the highest number of cybercrime (Du Toit, Hadebe & Mphatheni, 2018: 111). The economic crime survey conducted by Price Waterhouse Cooper in 2014 indicates that cybercrime has a negative impact on businesses, revealing that businesses lost more than 1 million US dollars in that year alone (Kader & Minnaar, 2015: 68).

According to Eziji (2014: 36), cybercrime bankrupt businesses, companies, organisations and individuals alike. Companies may close due to the inability to afford the salaries of employees, the slow operation of some companies makes them to be unable to grow the business, thus reducing or doing away with some of the benefits of workers like medical aids and failing to give employees market related increase annually. Eziji (2014: 37) further states that the cost of cybercrime to companies may be either direct, indirect or defence related. The direct cost relates to the hacking of people's bank accounts to withdraw their money illegally, indirect cost relates to people shifting to other banks due to loss of trust in a particular bank, while the defence cost is the cost incurred in the measures embarked upon to prevent cybercrime such as the installation of firewalls, antiviruses and other software programmes to detect and prevent hacking of computer systems.

Minnaar (2014: 128) argues that it is difficult to determine the precise impact of cybercrime because it is underreported to law enforcement and there is a lack of statistics to indicate the extent of this crime. Minnaar is supported by Ajayi (2016: 2) who states that cybercrime is a globally fast-growing crime that has a low detection rate with great returns for cybercriminals. It has an enormous impact on many people and countries worldwide. Minnaar (2014: 129) emphasises this by stating that it has a huge economic impact on individuals, businesses, companies and governments globally. He estimates that cybercrime costs the USA 38 billion USA dollars annually, in China the cost is estimated to be 37 billion USA dollars annually, in Brazil the estimate is 8 billion USA dollars annually, in South Africa it is estimated to be 3 billion USA dollars annually, while in New Zealand the cost is 2 billion USA dollars annually.

In 2013 the computer network of the South African Police Service was hacked and the information on whistle-blowers and victims of the police killings of striking mineworkers at Marikana got into the public domain (Van Niekerk, 2017: 118). According to Dlamini and Mbambo (2019a: 1), this type of crime has a negative effect on police operations of detecting, investigating and preventing crime because it makes it difficult for the public to trust the police and help them with the information they have. Their mistrust may be based on the fear that their identity might be revealed when systems are hacked. Failure to report some of these cybercrimes could be attributed to the fact that some people who have the means use their own cyber security measures to protect

themselves against cybercrimes, so they do not see the necessity of reporting these crimes to the police. This situation is compounded by the perceived failure of the police to protect themselves against such crimes and to deal effectively and efficiently with the reported crimes of this nature.

Mothibi and Amali (2018: 57) state that the higher education sector in China and Russia is one of the victims of cybercrime in which cybercriminals try to access university computer networks to steal information that will enable them to infiltrate nuclear research databases. In one instance students hacked the registrar's office to change examination results. This kind of cybercrime undermines the reputation of educational institutions and the qualifications that they offer. Such a crime compromises the academic quality of the affected institutions and negatively affects students who legitimately obtained qualifications at those institutions because potential employers and other educational institutions might question the authenticity of their qualifications. Ezeji (2014: 34-35) states that according to the South African cybercrime report published by Anti-Fraud Command Centre in 2011, more than 7000 phishing threat attacks had been detected in the country. In addition, the report indicated that it costs businesses approximately 52.3 million USA dollars annually and it takes 5-19 hours of phishing attacks on the computer network for 10 to 20 victims to provide the required personal information to cybercriminals, such as banking information, identity documents and credit cards.

South Africa, particularly the South African Police Service, is awaiting the coming into law of the Cybercrimes and CyberSecurity Bill. The Cybercrimes and CyberSecurity Bill (South Africa, 2016: 10-20) criminalises the hacking; unlawful interception of data; unlawful acts in respect of software and hardware tools; unlawful interference with data, computer programmes, storage mediums and computer systems; cyber fraud; cyber forgery; cyber uttering; and malicious communications. This Bill could empower the South African Police Service to deal with this crime effectively as Kempen (2019: 50) reiterates that the Constitution of the Republic of South Africa obliges the South African Police Service to combat, detect, prevent and investigate crimes, which includes cybercrimes. However, currently the South African Police Service does not have an approved integrated strategy framework that specifically deals with cybercrime. The police depend on common law, which spells out that fraud is

perpetrated online by means of computer networks connected to the internet and use other transgressions under section 86 to 88 of Electronic Communications and Transactions Act 25 of 2002. According to Schultz (2016: 13), prior to the enactment of the Electronic Communications and Transactions Act, the current law and legislation that deals with cybercrime failed to lead to effective arrest, detection, prevention and sentencing of offenders. It generally did not involve other stakeholders such as the police, private sector, academics and communities to forge partnerships to assist in combating cybercrimes effectively. Kempen (2019: 52) states that Intelligence-Led Policing can help police in strategic analysis to prevent and combat cybercrimes. It will enable the police to share information and intelligence related to cybercrimes and to connect/involve law enforcement with other stakeholders. The stakeholders might include security experts and non-law enforcement organisations that offer training to police to assist them in developing intervention strategies and to provide support on cybercrime investigations and digital forensics. It can also help them in sharing operational information, develop skills that can be used in dark web investigation, and enable them to interpret the trends and threats of cyber related crimes.

South African banks have been targeted by phishing schemes, the main target being credit card fraud, hacking bank accounts, identity theft, data loss and information leakage. These phishing attacks often occur through SMS swindle (Cassim, 2009: 63). Desai (2018: 153) cites an example of Liberty Holdings in which their computer system was hacked in 2018. In this process, the information of their high profile clients were removed from their system and a million rand was demanded from the company by cybercriminals for them not to expose that confidential information to the public. Cassim (2012:381-382) states that cyber terrorism is one of the most dangerous cybercrimes known in the world and cyber terrorists use computer networks to terrorise countries. Their main motive is to collapse countries' infrastructure, computer networks, financial systems, causing loss of life and destruction of properties etc. As an example of cyberterrorism, Cassim (2012: 385-386) cites a cyberterrorist attack in Sri Lanka in 1998 where terrorist groups, called the Ethnic Tamil Tigers Guerrillas hacked 800 e-mails of Sri Lanka embassies and then sent threatening messages that disrupted communication and threatened to kill people.

According to Cassim (2012: 396-398), the South Africa Police Service is currently policing cybercrimes through the following pieces of legislation, namely - the Prevention of Organised Crime Act 38 of 1999 (POCA), Financial Intelligence Centre Act 38 of 2001 (FICA), Electronic Communications and Transactions Act of 2002 (ECT) and Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA). Ezeji et al. (2018: 107) state that the POCA Act deals with the problem of organised crime, the FICA Act addresses the problem of the financing of cyber terrorism, the ECT Act deals specifically with cybercrime while the RICA Act compels consumers to register their mobile numbers with service provider networks, as required by South African law. According to Dlamini and Mbambo (2019a: 5-6), these sections of legislation that are used to combat cybercrime are ineffective. Given the fact that they were not specifically established to deal with cybercrime, they lack cyber security awareness and penalties imposed in relation to cybercrime matters. This legislation is not enough to deter the perpetrators of cybercrimes.

Intelligence gathering and spying have been used by the police for centuries to maintain control over the political motive (Zinn, 2011:13). Mashiloane (2014:32) elaborates by stating that such strategies have been used in various ways, such as fighting political battles in the ancient world, while modern intelligence is used for crime analysis, gathering information and research. Even though such intelligence has been seen as playing a pivotal role in combating crime years ago, it was not regarded as central to policing. Police managers have long been searching for something that can reveal the comprehensive picture of crime, but nothing has been shown to support the operational capability of the police department more than the use of intelligence in developing policing strategies (Kleiven, 2005: 258).

According to Canaday (2017: 21), the use of Intelligence-Led Policing can be traced back to the Kent Constabulary in the United Kingdom in the 1990s to respond to the high crime levels. It was commonly known as the Kent Policing Model and provided the basis of what we know as the Intelligence-Led Policing model today. The main objective of introducing Intelligence-Led Policing in the United Kingdom was to address the failure of the traditional reactive police style to deal with the rapid changes in globalisation that created the increased opportunity for transactional crimes. Its

implementation was focused on targeting offenders, identifying hot spots, understanding crime patterns for investigation of crime series and trends, and working together with crime prevention stakeholders to reduce crime (Govender, 2012: 83).

Bezuidenhout (2008: 54) states that Intelligence-Led Policing was used at an international scale for the terrorist attacks on the Twin Towers in the United States of America on 11 September 2001, the bombing of trains in Spain in 2004, and the bombing of the bus in the United Kingdom in 2005. Before the terrorist attack on 11 September 2001 in the United States of America, fewer than 30 countries were sharing crime information on possible terrorists, but after 11 September 2001, the number of countries sharing crime information on terrorists increased to more than 100. These countries were now working together on the identification of more than 10 000 people who were suspected of terrorist activities (Bezuidenhout, 2008: 54). Since April 2004 the use of Intelligence-Led Policing gained momentum in the United Kingdom as part of the policing crime combating strategy (Budhram, 2016: 80). This policing model can be used to combat cybercrime through risk assessment for content identification, intrusion detection, cyber intelligence gathering and cyber surveillance. It can also be used at all times to monitor the network system for interruptions as immediate responses to cybercrimes. It also forms part of cyber intelligence gathering and cyber forensic investigation to detect any cybercrime on the existing live connection from the suspect's network system to make it difficult for attacks by deflecting, disrupting and infecting attacking networks (Dlamini & Mbambo, 2019a: 7). During the 1990s this model was praised by policing experts in the United Kingdom and United States of America for its ability to combat crime. These experts saw Intelligence-Led Policing as an effective crime prevention model in the crime management philosophy and police practice (Budhram, 2016: 80).

In 1995 the South African Police Service adopted the use of Intelligence-Led Policing to combat crime and to address the problem of organised crime syndicates (Govender, 2012: 83). This model helps the police to understand the modus operandi during the commission of the crime through the collection and analysis of crime information. The use of Intelligence-Led Policing is proactive to help the police to develop tactical responses after understanding crime information and changing threats (Mashiloane, 2014: 172). Intelligence-Led Policing combats cybercrime by being aware of the

modus operandi of attackers, their motives, networks and capabilities of attacking. Intelligence gathering and sharing crime information with private stakeholders and international policing agencies play an important role in combating cybercrime (Fick, 2019: 3). This model can help police to share information and intelligence to recognise the role of cybercriminals during the commission of crime. This information and intelligence can be collected, analysed, interpreted, verified, packaged and disseminated in such a way that it can be used for awareness campaigns and intelligence to conduct investigation to combat cybercrime (Kempen, 2019: 54). It can also be used in surveillance to record the movement of cybercrime, investigate and record illegal financial dealings and to link the cybercrime networks for direct police observation of online threats (Zinn, 2011: 15).

The use of Intelligence-Led Policing to combat crime was subsequently endorsed across the world as an effective crime prevention strategy (Ezeji, 2017: 196). Intelligence-Led Policing is a police business model that directs them to collect, analyse, organise and utilise crime information systematically for the operational, tactical and strategic planning to combat crime including cybercrimes. The police use this model to collect, examine, and compare crime information to identify crime patterns, identify criminals, their associations and scene of incidents of cybercrime (Ronczkowski, 2012: 115). Matsaung (2019: 56) emphasises that this model should be used in a way that produces evidence that could lead to the successful prosecution of cybercriminals.

1.3 PROBLEM STATEMENT

The threat of cybercrime has created distress/alarm in individuals, governments, businesses and security agencies, forcing them to implement stringent cyber-security preventive measures to prevent a network of cybercriminals in cyberspace. The use of meta-data like cell-phone messages and digital photographs increases the source of information for collection and selling. According to Dlamini and Mbambo (2019a: 10), cybercrime, with the increased use of technology becomes more threatening every day in South Africa. The sophistication in which technology is used to obtain and manipulate information is a real challenge to the police, while the non-physical boundaries of this crime as compared to traditional crimes, complicate its policing in terms of its detection, combating and investigation.

Mothibi and Amali (2018, 58) state that South Africa is one of the developing countries in Africa with a very high number of cybercrimes. This could be attributed to the higher industrialisation and the growing number of unemployment in the country, particularly within the youth. They (cybercriminals) engage in illicit computer activities such as identity theft, cyber bullying, e-commerce fraud, online child pornography and hacking. Kempen (2017: 59) states that South Africa loses almost two billion rand annually due to internet fraud, phishing and hacking. According to Kempen (2019: 50), the South African Police Service does not reflect cybercrime in its crime statistics, because victims of this crime do not report it to the police and some victims only realise that cybercrime has been committed against them after some time. They only get to know about this when they are informed about outstanding debts that occurred through the fraudulent use of their personal particulars or when they are told that they have been blacklisted. Ezeji (2014: 38-39) indicates that cybercrime costs South Africa an estimated amount of R 412 million per annum, of which the amount of R110 million is not recovered by the law enforcement. The causes of the high volumes of cybercrime include the internal growth of businesses, the higher numbers of mobile internet users, lack of awareness campaigns of cybercrime and increasing unemployment. The criminal justice system needs to put security measures in place to ensure that cybercrime is tackled effectively. The general society must be informed through national awareness campaigns about the danger of cybercrime. It is of the utmost importance that people are aware of the trends and the manifestation of cybercrime in South Africa.

Desai (2018: 152) states that the financial sector and bank institutions have become the targets of cyber-attacks that cost their businesses immense amounts of money. In 2016 one of the largest cyber-heists in history of cybercrime occurred when the Central Bank of Bangladesh lost almost US\$81 million and the money was transferred via online banking to the Philippines through a casino system. According to Mpuru (2017: 44), the report published by the National Cyber Security Hub (Council for Scientific and Industrial Research) indicates that between 2011 and 2015 there had been more than 6000 cyber-attacks in South Africa directed at critical infrastructure, business and internet providers. Kader and Minnaar (2015: 68) point out that the increasing number of cyber-attacks puts internet users at serious risk because they

use social networking sites as platforms for communication, meeting people, sharing ideas and business transaction on a daily basis.

According to Du Toit et al. (2018, 119), the South Africa Police Service largely uses common law which criminalises corruption via the falsifying of invoices through the internet. The police also employ the Electronic Communications and Transactions Act No 25 that deals with electronic transfer of money and illegal access to information. This legislation appears to be ineffective, because it is difficult to locate where this crime has actually been committed and where the perpetrators are situated to be able to arrest them. The failure of the police to use Intelligence-Led Policing intensively could also be another factor that hampers their success in terms of following the trails of the criminals, and providing solid evidence that should lead to their successful prosecution.

The above section indicates that cybercrime and cyber security in South Africa is currently dealt with by different pieces of legislation and common law that develop on a case-by-case basis. In reality, however, the Electronic Communications and Transactions Act (ECT) 25 of 2002 has been regarded as ineffective in dealing with cybercrime. Schultz (2016: 29) states that it is difficult to prosecute offenders successfully and to impose effective penalties on those who are convicted to deter others from committing cybercrime through the ECT Act. The Act states that a person found guilty of cybercrime can be imprisoned for a period not exceeding twelve months or a fine in terms of section 89(1). Alternatively, a fine or imprisonment not exceeding a period of five years in terms of section 86(4); 86(5); or 86(7); which Schultz (2016: 29) argues are not heavy enough to deter people from committing these crimes. This argument gives credence to the need for specific cyber laws in South Africa that could expedite the prosecution of cybercriminals and impose harsher penalties that could deter others from committing these kinds of crime.

Ntsaluba (2017: 61) also stresses a jurisdictional matter as a shortcoming of the ECT Act in the fight against cybercrime, by stating that it focuses only on people who committed cybercrime within the Republic of South Africa and excludes those who committed crime outside the country. Sections 80-84 deals with the appointment and responsibilities of cyber inspectors to monitor, inspect, search and seize crime

information related to cybercrimes, but unfortunately are only empowered to issue enforcement and compliance orders.

The Cybercrimes and CyberSecurity Bill of 2016 that has been passed by the National Assembly must still be passed by the National Council of Provinces and it is hoped that it will deal with crime and criminality in cyberspace. According to Schultz (2016: 35), the Bill will address the shortcomings of the ECT Act by increasing the penalties, as people who will be found guilty of cybercrime could be sentenced to a minimum period of five years and the maximum period of ten years imprisonment. Fines could range from five to ten million rand. The Bill also attempts to bring a collaborative effort by bringing on board institutions such as the National Cyber Centre, Cyber Command Centre, Government Security Incident Response Team, Security Hub and Private Sector Security Incident Response Teams to be part of the structures that will deal with cybercrime.

Phahlamohlaka and Hefer (2019: 3-6) provide the following analysis of some of the functions of the cyber security centre, cybercrimes centre, cybersecurity hub and cyber command as contained in the Cybercrimes and CyberSecurity Bill of 2016.

Cyber Security Centre: this centre will facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange on national security and threats to improve technical response coordination. Secondly, it will develop rules to guide coordinated responses to cybersecurity incidents and interaction with the various stakeholders. Thirdly, it will ensure that cyber security audits, assessments and readiness exercises are conducted and will provide advice on the development of national response plans.

In providing the analysis of the Cyber Security Centre, Phahlamohlaka and Hefer (2019: 3) indicate that obtaining acceptance from some communities would need innovative approaches, because these communities may not be aware that a cyber-incident that requires coordinated response has occurred in their vicinity. They explain that this requires vast human and material resources not only from the Cyber Security Centre, but from all these four structures, namely - cyber security centre, cybercrimes centre, cybersecurity Hub, as well as the cyber command.

Cybersecurity Hub: this hub has to coordinate general cyber security activities in the private sector. Additionally, it has to inform the Private Sector Security Incident Response Teams, electronic communications service providers, vendors and other persons or entities who have an interest in cyber security, of the developments in cyber security. Thirdly, it has to initiate cyber security awareness campaigns. Fourthly, it should encourage and facilitate the development of Private Sector Security Incident Response Teams, and lastly, conduct cyber security audits, assessments and readiness exercises on request.

The analysis by Phahlamohlaka and Hefer (2019: 4) reveals how the hub is very well positioned to initiate cyber security campaigns and activities for civil society and private sector, thus stimulating viable social activities.

Cyber Crimes Centre: this centre–facilitates the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange on law enforcement, as well as threats in order to improve technical response coordination. Secondly, to develop response rules to guide coordinated responses to cybersecurity incidents. Thirdly, to develop and maintain cross-border law enforcement cooperation on cybercrime. Fourthly, to facilitate the establishment, promotion and maintenance of the public-private cooperation in fighting cybercrime. Lastly, for the establishment, promotion and maintenance of international cooperation in the fight against cybercrime.

Phahlamohlaka and Hefer's (2019: 5) analysis indicates that unlike conventional crime incidents, cybercrime incidents may happen all at once in one location, thus making it almost impossible for the community to report observed incidents.

Cyber Command: to facilitate the coordination of cyber security incident responses on national defence. Secondly, to develop measures to deal with cyber security matters for the national defence. Thirdly, to facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange and threats on national defence. Fourthly, to ensure the conducting of cyber security audits, assessments and readiness exercises and provide advice on the development

of national response plans on national defence. Phahlamohlaka and Hefer (2019: 6) state that the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange and threats on national defence improve technical response coordination and develop measures to deal with cyber security of the national defence.

Reddy and Minnaar (2018: 78) point out that the Japanese-based Gox Company, the largest Bitcoin Exchange Company in the world was hacked and lost 473 million US dollars in 2014. The perpetrators accessed the computer system and stole the private key that was password protected to manage the virtual wallet stored on cryptocurrencies, they then used this key to open a wallet and steal crypto-currencies. The main reason for targeting the Bitcoin Exchange Company was to take over the cryptocurrencies mining pool and the computing powers. The modus operandi used by the hackers was to infect viruses into the mining system to gain access to the private key that was stored on their system to enable the hackers to get access on the mining pool account and change the payments method system addresses to pay directly to their own accounts. Reddy and Minnaar (2018: 79) further state that hackers target mining pools to create dark web (dark web refers to invalid websites, visible to public and Internet Protocol addresses which remain anonymous and no link can trace the servers) marketplaces to open fake websites on various online marketplaces in order to post the links on a number of dark web marketplaces, and once victims log on the links, their usernames and password are directed to the hacker. Once cybercriminals have hooked the victims, they monitor the mining pool accounts of the victims at all times and once the money has been deposited, the hacker withdraw it before the victims can have access to it (Reddy & Minnaar, 2018: 79).

According to Staff Writer (2018: NP), in 2018 more than 27 500 people who were affected by cybercrimes on their crypto-currencies mining pool were Americans, South Africans and Australians who were scammed out of an estimated R16 000 to R 1.4 million of investments with a forex trading company, BTC Global. There is an indication that the amounts could be higher if more victims who had lost money through investing in the crypto-currencies mining pool could come forward. Staff Writer (2018: NP) further states that the Directorate for Priority Crime Investigation (DPCI) launched an investigation into crypto-currencies to catch culprits, but unfortunately their

investigation did not yield results because it could not reveal whether it is a Ponzi (a Ponzi scheme is a fraudulent investing scam which generates returns for earlier investors with money taken from later investors) or a pyramid scheme (a pyramid scheme funnels earnings from those on lower levels of an organization to the top, and are often associated with fraudulent operations). It was also not possible to determine the nationality of culprits.

Reddy and Minnaar (2018: 87) maintain that the failure of the police to utilize Intelligence-Led Policing to combat cybercrime effectively results in the slow response of the police to break down the anonymity, to identify the Internet Protocol (IP) address and the location of these crimes. In addition, this failure (to use Intelligence-Led Policing) has a ripple effect, because it contributes to the failure to make physical arrests, the inability to trace money that has disappeared in one location and then reappears in another, as well as the failure to identify hidden transaction activities operative on the dark web. According to Kader and Minnaar (2015: 73), the police would use traditional law enforcement to combat cybercrimes rather than use Intelligence-Led Policing that can cope and successfully deal with the detection, investigation and prosecution of cybercrimes.

According to Ezeji (2014:4), the common modus operandi used by cybercriminals to access computers (hacking) is to attach worms to normal files such as e-mails and when the victim opens the link, viruses are automatically transported to their computer systems which damage them. The intention is to gain access to the private computer with the aim of deleting financial records of companies, accessing e-mails, destroying sensitive information or sabotaging the company computer system. The ultimate aim is to steal financial information of the company, to blackmail the company, to sell company information to other criminal group networks or to create fraudulent credit cards (Maras, 2015:7). Phishing which aims to deceive individuals to provide the offenders with their personal information in the belief that it comes from legitimate established enterprise, is also common in South Africa (Reddy & Minnaar, 2018: 80). According to Ezeji (2014: 80), the South African Revenue Service became one of the victims of phishing between January 2013 and February 2014 when cybercriminals attacked their websites, deceiving taxpayers by sending them fake refund notices and appropriating the tax refunds for themselves.

Veerasamy (2017: NP) affirms that cyber threat intelligence plays an important role in combating cybercrime because the police can identify and attempt to understand threats to investigate the source, motivation and capabilities of the attackers. It helps the police to be aware of the threats and vulnerabilities on the network system to minimize the online threat and to limit the access of cybercriminals to the network. It also helps to respond to cybercrime effectively as a counter measure attack to contextual information about the cybercrime which includes techniques, tactics, patterns, indicators, actors and locations of the crime. The purpose of cyber threat intelligence is not only to detect, identify and stop attacks, but it is also to determine who is attacking, how the attacks are being implemented, who is a possible target and its location. According to Veerasamy (2017: NP), the police can understand cybercrime better through the use of cyber threat intelligence such as Signal Intelligence, Open Source Intelligence and Human Intelligence. The aim of Signal Intelligence is to identify the incoming data into the network, Open Source Intelligence helps to produce large quantities of cybercrime information that provide threat alerts, while Human Intelligence is used as surveillance to detect emerging trends and threats. Ezeji and Olutola (2018: 186) state that the use of cyber forensic and cyber intelligence as products of Intelligence-Led Policing can help to combat technological crimes such as cybercrime through developing intelligence professionalization programmes that uplift skills of police officers to prevent and investigate cyber-related crimes. It should ultimately ensure access to intelligence training for innovation on how to use technology and share information in combating cybercrime.

According to Zinn (2011: 10), the ineffective and reactive policing styles used by the South African Police Service to control and manage crime could largely be blamed for the high crime levels. Some of these high crime levels could be attributed to the failure to utilise Intelligence-Led Policing that is internationally recognised as an effective crime prevention model. It is the responsibility of the police to share crime problems with other law enforcement agencies and other relevant stakeholders to help them to control crime. This seemingly unwillingness creates the impression that the police maintain their isolationist culture by closing ranks in order to avoid criticism from other stakeholders who might be critical of the manner in which they are dealing with crime in the country. Budhram (2016: 85-86) supports this sentiment by stating that police

failure to use Intelligence-Led Policing could largely be blamed for the increased opportunities for criminals to commit organised transnational crime, which poses physical and technological challenges across policing. The physical challenges refer to the fact that the police use reactive police models such as sector policing, community policing, problem-oriented policing and partnership policing, limiting their ability to deal and cope with the increased organised transactional crime.

Ezeji and Olutola (2018: 169) indicate that some police officers do not utilise Intelligence-Led Policing because of their lack of understanding of its value in crime prevention and crime combating, underestimating its true value of collecting a large volume of data, identifying crime hot spots, analysing and disrupting crime. Budhram (2016: 89) further states that the use of Intelligence-Led Policing in South Africa is hampered by the complexity of the policing environment, where the private and public organisations are only allowed to do business intelligence by collecting information for tactical and operational use. Under no circumstances can they collect strategic intelligence information because it is only the South African Police Service that is authorised to conduct strategic intelligence to perform its functions that are set out in section 205(3) of the Constitution of the Republic of South Africa of 1996 and in terms of the National Strategic Intelligence Act No 39 of 1994.

Unlike community and sector policing that have directives and guidelines from provincial and national level on how they should be implemented, there are no such guidelines and directives for Intelligence-Led Policing (Mashiloane, 2014: 261). The reason for the South African Police Service not to have guidelines on Intelligence-Led Policing is because the implementers have diverse comprehension of what constitutes intelligence; some regarding it as a secret that could easily be associated with a negative connotation of subversive activities. Some implementers regard it as a marginalised, subordinate and furtive activity that becomes central to contemporary policing (Ezeji, 2017: 192-193). The lack of policy framework on Intelligence-Led Policing also contributes to the misunderstanding of its conceptual framework, resistance and rejection by some police officers to use it, as well as the lack of training among police leadership and officials who must implement it (Ezeji: 2017: 357).

According to Kader and Minnaar (2015:80), the effective combating of cybercrimes requires law enforcement agencies that do extensive and in-depth research on cybercrimes to know how to investigate, apprehend and prosecute such criminals. Such research will enable them to identify cybercrime attackers, their motives, the resources that they use and their modus operandi. Fick (2019: 32) reiterates the value of Intelligence-Led Policing in detecting, preventing and investigating cybercrime. According to Kempen (2019: 54), the use of Intelligence-Led Policing in combating cybercrime will assist police to monitor cybercrime- related incidents online at all times throughout the year. It will also help to be on the lookout for any illegal activities that might occur online for early detection, investigation and apprehension. The continuous flow of information and intelligence can be used to deal with cybercrime to identify other stakeholders such as banks, internet service providers, international police organisations and the public. This crime prevention approach can help police in the collection, analysis and interpretation of evidence that may lead to the identification of online threats to combat cybercrime.

1.4 RESEARCH AIM AND THE RESEARCH OBJECTIVES

According to Dawson (2016:292), the aim of the research is the overall driving force of the research project. It is the main goal or overarching purpose of a research project (David & Hodges, 2010:38). Therefore, the research aim of this study is to understand the use of Intelligence-Led Policing in combating cybercrimes in South Africa.

Conversely, research objectives are the goals that the researcher wants to achieve at the end of the study. According to Creswell and Creswell (2018: 117), research objectives indicate the reason for conducting the study, the direction it takes and results it intends to achieve. Newman, Ridenour, Newman, and De-Marco (2003) mention the possible nine reasons for conducting the research as improving prediction; increasing the knowledge base; having a social, organizational or institutional impact; measuring change or improvement; helping one understand complex phenomena; testing and evaluating new ideas and theories; generating new hypotheses and theories; informing multiple stakeholders; and understanding past events. The following objectives have been developed to achieve the aim of the study:

- To establish the extent to which Intelligence-Led Policing is used to combat cybercrimes.
- To establish the value of Intelligence-Led Policing in combating cybercrimes in South Africa.
- To determine the challenges encountered by the police in the use of the Intelligence-Led Policing in combating cybercrimes in South Africa.

1.5 RESEARCH QUESTION

Newman and Covrig (2013:70) state that consistency in the title, problem, purpose, and research question improves the logic and transparency of the research project. When these components are aligned and more coherent, the research report is more comprehensible. Newman and Covrig (2013:75) opine that the research question emanates from the title, as it indicates the need and the significance of the study. The research question informs the reader what the researcher will do to fill the gap in the research or to solve the problem. In a nutshell, the research question refers to a statement that organises, gives direction, delimits and clarifies the boundaries of the research study (Punch, 2005: 37). It creates the focal point of the study and outlines the important concepts that need to be studied (Bless, Higson-Smith & Sithole, 2013: 71).

At the backdrop of the above, the main, research question for this study is as follows: How is Intelligence-Led Policing used to combat cybercrimes in South Africa? Based on this main question, the following sub-question has been designed to facilitate the answering of the main question, namely - What challenges are encountered by the police in the use of Intelligence-Led Policing to combat cybercrime in South Africa?

1.6 THE SIGNIFICANCE OF THE STUDY

Research contributes to the investigation of the prevailing challenge or problem with the ultimate aim of addressing the existing gaps in the literature. On the other hand, research plays an important role in developing theory and disseminating knowledge to communities at large (Gray, 2018: 3). According to Richardson (2000: 254), research by its nature may lead to new discoveries, better understanding of concepts or phenomena, thereby making a theoretical contribution to a discipline. The significance of the research study should be judged by factors such as its ability to

extend knowledge, to improve practice, generate ongoing research or empower communities.

Tracy (2010: 846) categorises the significance of the study into the following:

- *Theoretical significance* - The research basically provides a theoretical contribution by examining how existing theories or concepts may contribute to the understanding of a new phenomenon in a different context. It emphasises that the theoretical significance requires more than the mere application of existing theories, because it should build on existing theories or problematize current theoretical assumptions. An effective study should build on past research to provide new conceptual interpretations that can be used by future researchers. Conceptualisation helps explain social life in different ways, which enables the study to build on previous studies and provides new conceptual understanding.
- *Heuristic significance* – This refers to the ability of the research to develop curiosity that inspires readers to explore further research because it provides readers with substantive and interesting suggestions for future research. Therefore, it should influence various audiences, such as policy makers, research participants, or the lay public.
- *Practical significance* – deals with the usefulness of the knowledge and its ability to shed light and empower participants to see the world from different perspectives. Good qualitative research should supplement and complement rather than displace attempts to deal with challenges. It serves to capture how practitioners cope with challenges and provides and provides measures that could help to deal with challenges.
- *Methodological significance* – relates to the ability of the research to provide a contribution by introducing and explicating a new methodological approach. This could lead to theoretical insights and practical useful methods of explaining a certain phenomenon.

Positioning the significance of this study in relation to the aforementioned categories need to be understood within the context of high levels of cybercrime and the role that Intelligence-Led Policing plays or should play in dealing with such crimes. The high crime rate in South Africa is a serious concern for both public and private stakeholders (Budhram, 2016, 80). According to Ezeji (2014: 2), the South African criminal justice system is struggling to understand the dynamics and complexity of cybercrimes. This research focus constitutes exploring the role of Intelligence-Led Policing in combating cybercrime in South Africa. It will contribute to the criminal justice system in South Africa by introducing cyber intelligence and cyber security measures that can help to monitor and prevent cybercrime, thus providing theoretical and heuristical significance to the role of Intelligence-Led Policing in the policing of cybercrime. It will also benefit academics and students to identify research gaps on the policing of cybercrime and stimulate future research on the topic. It may also assist in alerting communities at large on how to safeguard their mobile phones and computers by regularly updating them with anti-spyware programmes to protect themselves against cybercriminals. Furthermore, this study will help government, business, banks and companies on how best to detect and combat cybercrimes, thereby being of practical significance to policing.

1.7. DEFINITION OF CONCEPTS

A concept is a building block of research studies, as it represents an object, a property and a certain phenomenon (Welman, Kruger & Mitchell, 2005: 20). Every research study has its own specialized language and concepts that are used to guide the reader to understand the context of the research study (Montesh, 2019:18). The following concepts are used in this study:

1.7.1 Intelligence-Led Policing - Intelligence-Led Policing is a business model for planning police activities and directing resources for data analysis, prevention, problem reduction and the disruption of crime through strategic management and effective enforcement strategies to target prolific and serious offenders (Budhram, 2016: 81). It is basically the collection, processing, analysis and use of crime information to plan police operations in preventing and combating crime. According to Ratcliffe (2008:13), it is a policing approach that targets prolific offenders, triage out

the unsolvable crime, more strategic use of informants, and make decisions based on the prevailing intelligence analysis.

1.7.2 Cybercrime – Cybercrime refers to crime perpetrated with a computer via the internet, thus making the computer a tool to commit crime anywhere in the world (Mothibi & Amali, 2018: 57). Du Toit et al. (2018: 113) define it as unethical behaviour to gain access to a computer system without authorisation to transfer or destroy data. Van Rensburg (2018: 2) gives an extended definition by defining cybercrime as an act of criminality that takes place on a computer, mobile phone, tablet or computer network thus rendering these gadgets the origins of the crime scene.

1.7.3 Phishing - Phishing is the sending of untrustworthy information to victims to steal their personal or confidential information (Van Rensburg, 2018: 3). Reddy and Minnaar (2018: 80) define it as an internet scam that uses social engineering tactics to defraud victims by sending deceiving e-mail communication.

1.7.4 Malware – Malware is any malicious software programme designed to disrupt and damage the operations of the computer system (Ezeji et al., 2018: 97). It is often called computer viruses, used to attack computer systems to disrupt its operation, gain the access to it and steal sensitive information (Ezeji, 2014: 31). Malware is a comprehensive term for malicious software such as viruses, worms, trojans and other harmful computer programmes used by hackers to access sensitive information to cause extensive damage to the data and the computer system or to gain unauthorised access to a network.

1.7.5 Hacking - Hacking is to deliberately transfer viruses into the computer network to witness its operations with the intentions to access its databases for various purposes such as copying, deleting and transferring information to sell it (Minnaar, 2014: 132). It is a covert technical ability to gain access to a computer network system for risk and threat assessment testing (Reddy & Minnaar, 2018: 78). Basically, it relates to the exploitation of the computer system to gain unauthorised access for illicit purposes.

1.8 RESEARCH DEMARCATION

Research demarcation means that the researcher focuses on the specific area of study to ensure that the research study is researchable and manageable. According to Silverman (2000: 88), research demarcation involves the selection of an area, sampling of a group of people or the identification of the phenomenon to be studied in order for the study to have a limited scope and be more manageable. There is no way that a research study could focus on the entire population because in that case the study could be unmanageable. This study explores the use of Intelligence-Led Policing in combating cybercrime in South Africa. The study was conducted in South Africa within the South African Police Service and the Directorate for Priority Crime Investigation as they are the policing agencies that deal with criminal activities including those that are related to cybercrime.

South Africa is made up of nine provinces and the empirical research was conducted in only 5 of the 9 provinces. The 5 provinces were Limpopo, Gauteng, North West, Free State and Mpumalanga, because they experience higher incidents of cybercrimes and they comprise mixture of urban and rural provinces, thus representing the demographics of South Africa.

The South African Police Service's functional activities are carried out by the Uniform Branch and the Detective Branch. The study focused on the detectives who deals with cybercrime and crime intelligence members. While for the Directorate for Priority Crime Investigation the focus was on members who deal with cybercrime. Both these, members from the South African Police Service and the Directorate for Priority Crime Investigation are deemed to have intimate knowledge and experience how Intelligence-Led Policing is used to combat this crime.

1.9 ORGANISATION OF THE THESIS

Chapter One: General Orientation - This chapter provides the introduction, background of the study, problem statement, research question, research objectives, significance of the study, theoretical concepts and research demarcation.

Chapters Two to Five comprise the Literature Review

Chapter Two: Cybercrime in South Africa - This chapter deals with the historical context of cybercrime. It covers types of cybercrimes in South Africa, challenges, risk, consequences and prevalence of cybercrime.

Chapter Three: The use of Intelligence-Led Policing to Combat Cybercrime - This chapter focuses on the evolution of Intelligence-Led Policing, its practical implementation, as well as comparative Intelligence-Led Policing in different countries and the intelligence process.

Chapter Four: International Perspective on the policing of Cybercrime and Intelligence-Led Policing - This chapter discusses the ways in which different countries deal with cybercrime, the measures used to deal with cybercrime and the effectiveness of cyber laws.

Chapter Five: The use of Crime Analysis to Combat Cybercrime - This chapter deals with the role of the criminal justice system in combating cybercrime. It explores the prevention, investigation, and the prosecution of cybercrimes.

Chapter Six: Research Methodology - This chapter focuses on research methods, namely - research design, population and sampling of the study, data methods, data analysis, validity and reliability of the study as well as trustworthiness of the study and ethical considerations.

Chapter Seven: Presentation, Discussion and Interpretation of Research Findings - This chapter represents, interprets and reports the findings of the study.

Chapter Eight: Recommendations and Conclusion - This chapter provides the recommendations based on the findings of the study to address the identified shortcomings and a conclusive view of the entire study.

1.10 CONCLUSION

This chapter provided an overview of cybercrime, its negative economic impact on South African citizens in terms of revenue lost due to cybercrime and the challenges

experienced by the police in combating such crimes. The legislative challenges in effectively dealing with cybercrime and the challenges with current punitive measures that do not seem to act as deterrents to offenders and potential offenders of these crimes were also scrutinised. The background regarding the use of Intelligence-Led Policing to combat crime in general and how it could also be used in cybercrime is also evident from the literature reviewed in this study. An overview of how Intelligence-Led Policing may be used in combating, detecting, preventing and investigating cybercrime in South Africa was also provided.

This chapter outlined the contribution that could be made by the use of Intelligence-Led Policing in dealing with cybercrime through the involvement of essential stakeholders in the criminal justice fraternity by introducing cyber intelligence and cyber-security measures that could be used in monitoring and preventing cybercrime. The concepts that are used in this study are also defined to enable the readers to understand the context of the study and the direction it takes. Indicated in this chapter is also the demarcation of the study that shows the area that was delineated by the empirical research in South Africa as an empirical study cannot be conducted in the entire country. The subsequent chapter will focus on the policing of cybercrimes, types of cybercrimes in South Africa as well as their challenges, risks, consequences and prevalence.

CHAPTER TWO: CYBERCRIME IN SOUTH AFRICA

2.1 INTRODUCTION

The prevalence of 'new' kinds of computer crimes can be likened to the proverbial cat and mouse game between the police and the criminals. It seems as if the new mice, the botnet attacks, ransomware, phishing, distribution of denial of service, voice-over internet protocols and geo-locative software pose new menaces, indicating that cybercrime will always be around. Until very recently cybercrime was unknown or underestimated by law enforcement agencies around the world, but it is now posing serious threats to information systems (Buono, 2012:332). It is one of the biggest topics discussed around the world as it poses serious threats to Information Communication Technology (ICT) in developed and developing countries (Kundi & Akhtar, 2014: 65). Cybercrime affects many citizens around the world, as it does not only occur via the internet and it can also take place through hi-tech industries and businesses, thereby affecting ordinary members of all walks of life. It has become one of the global problems that is staggering in its proportions, also because it includes other elements of different types of crimes and categories that link with threats that are perpetrated on the cyberspace, namely e-fraud crime (Minnaar, 2014: 128). Cybercrime does not involve physical conduct in which criminals carry AK-47s and blowup vans transporting cash, but it is a crime where criminals use computers as a weapon by simply clicking a mouse (Desai, 2018: 150). The threat of cybercrime forces many businesses, governments and security agencies around the world to implement stringent preventive measures to guard against any cyber threats in cyberspace (Desai, 2018: 154). Like in many other countries, cybercrime has become a serious challenge in South Africa, and that is why the South African Government introduced cybercrime legislation such as Electronic Communications and Transactions Act 25 of 2002 (ECT) and the Interception of Communications and Provision of Communication related Act 70 of 2002 (RICPCIA) to combat cyber-related crimes (Mothibi & Amali, 2018:57).

It appears as if the existing laws are not effective in dealing with cybercrime in South Africa. The police seem to be overwhelmed by the nature and magnitude of cybercrime that knows no borders, making it possible to be committed anywhere in the world. This current situation emphasises the need for international cooperation between countries

to deter, investigate and prosecute cybercriminals. Basdeo, Montesh and Lekubu (2014: 48-49) state that to combat cybercrime successfully, law enforcement agencies should not be limited by sovereignty and jurisdiction. Kempen (2019: 51-52) indicates that the challenges to deal with cybercrime compelled senior SAPS police officers to visit the Europol and Europol Cybercrime Centre in the Netherlands in 2018, seeking advice on how to deal with cybercrime. This visit assisted the SAPS in learning the best practices that could be included in the development of their policy framework in combating cybercrime.

2.2 THE OVERVIEW OF CYBERCRIME

Cybercrime is a challenge for law enforcement agencies, academics and cyber-security experts in the digital space all over the world in the 21st century (Moskowitz, 2017: 3). According to Maras (2015: 2), cybercrime does not have physical and geographic boundaries because the internet provides the opportunity for cybercriminals to meet other electronic device users in cyberspace via computer networks around the world. Moskowitz (2017: 4) reaffirms that cybercrime occurs in various ways such as hacking that seeks to exploit the weaknesses of computer networks for profit or political motives. Phishing is a form of hacking in order to steal personal and sensitive information and spamming is also used to infect the computer network of others by posting unsolicited communication. According to Mothibi and Amali (2018: 59), cybercrime is an offence against ICT systems whereby crimes can be committed in cyberspace through the internet. Most crimes that are committed in cyberspace are financial crimes, followed by other crimes such as human trafficking, extortion, theft of identity numbers, child pornography, blackmail, pimping and prostitution. Worldwide, most cybercrime incidences are committed by organised criminal networks which operate underground and their operations are well-structured to perpetrate unlawful acts against their victims, leaving them in vulnerable situations.

Minnaar (2013: i) states that to commit cybercrime, cybercriminals use a variety of techniques such as email scams to obtain personal information, theft of identity and bank account details for financial gain. Hackers access computer databases to steal information by means of cyber-ransom, cyber-fraud, and theft of intellectual property and cyber-blackmail with the ultimate aim of defrauding people. Ortmeier (2013: 144) states that the use of the internet creates vulnerabilities of computer networks all over

the world. The internet is now the preferred tool for sharing information amongst individuals every day and cybercriminals take this opportunity to infect viruses on computer networks to gain access to databases for theft of information and denial of service.

According to Minnaar (2014: 127-18), many people have connected their lives, both personally and professionally to digital platforms and that is why cybercriminals are interested in getting their personal information to exploit them. The expansion of cyberspace, together with the increase of broadband internet connections, powerful Wi-Fi connections, the use of mobile phones and technological devices create increased vulnerabilities to information systems and cloud computing. Boyd (2014: NP) indicates that the increasing exploitation attacks by cybercriminals, foreign nationals looking for sensitive data, or organised crime groups and terrorist groups committing other financial crimes making threats go undetected for months. Minnaar (2014: 128) argues that the information stolen on cyberspace is not only financial data, but terrorists and rogue governments can further their political agendas by stealing confidential data such as intelligence information to expose a country and harm potential citizens.

According to Du Toit et al. (2018: 113), phishing is a form of cybercrime in which cybercriminals create fraudulent websites to trick victims to reveal their personal information online, and once it is provided the attackers use that data to commit electronic fraud. South African citizens are victims of cybercrime because cybercriminals launch attacks using Trojan horse, a programme which is seen as normal to victims, but in reality it is malicious software that use backdoors to gain access to networks which later gives them the opportunity to access the network to launch attacks on the victims' computer systems. Cybercriminals can also use viruses (malicious software) to hack computers by transporting viruses by means of different approaches such as via emails and instant messages with a link (Ezeji et al., 2018: 97). Cybercrime can be found anywhere in the world, targets organisations, governments, banks, and social network users for data breaches, fraud, cyber stalking and phishing. Even if those targeted have cyber-security measures in place, cybercriminals find ways to neutralise their computer security to gain access (Desai, 2018: 150). The outbreak of the global Coronavirus pandemic increased cyber-attacks

when cybercriminals saw opportunities for exploiting victims through various attacks such as phishing in the form of business email compromises, fraud scams and implanting malicious software such as malware, spyware and ransomware on the computer systems of companies, organisations and individuals via the internet to exploit victims financially. Cybercriminals committed COVID-19 related fraud such as selling fake online medical supplies, tricking victims into buying counterfeit COVID-19 medicines, selling coronavirus testing kits, forming non-profit organisations, or claiming to fight pandemic by developing vaccines to combat the COVID-19 virus (Minnaar, 2020: 31).

2.2.1 Cybercrime Categories

Hacking is regarded as a long-standing form of cybercrime and it is designed to break into computer systems or network systems to have access for the assessment of risks and threats in computer systems. It includes any activities that can be used to gain backdoor access to computer systems with the intent to destroy information, steal information and make changes on websites (Reddy & Minnaar, 2018: 78). It weakens the computer security to exploit and hijack remote sessions of computers or obstruct the intimate knowledge of networks and computer operating systems to gain access to legitimate users' computer systems (Easttom & Taylor, 2011: 10).

2.2.1.1 Hacking and the hackers

Hacking involves unauthorised access to computer networks with the intention to damage it, its contents or to steal information (Maras, 2015: 6). It basically compromises computer security through unauthorised access and intentionally planting viruses or manipulating other computer networks to gain access and steal information for various purposes such as blackmailing, financial benefits, sabotaging and destroying other computers. Hacking comprises unauthorised access to a computer network to destroy information, alter information, steal information or to effect changes to the hardware (Reddy & Minnaar, 2018: 78). A hacker possesses expert knowledge on computers as well as the ability to exploit other people's computer systems by disrupting them with malicious software programmes to bypass antiviruses, security kits and high-end encryption of firewalls (Minnaar, 2014: 132). Ezeji et al. (2018: 96) state that hackers target computer systems to exploits its weaknesses and gain unauthorised access for malicious intent. They use port

scanners to check the weaknesses of the networks and to identify vulnerabilities that could enable them to access those networks. They use port scanners to determine whether there is any port in the computer that is open or available which can then be targeted to access computer networks. Once hackers have access to the networks, they crack passwords using methods such as packet sniffers which are used for capturing data on computer networks. These hackers use password- cracking as methods to recover passwords and other data found on computer networks (Ezeji, 2014: 29).

2.2.1.2 Types of hackers

Individuals who engage in hacking sometimes come from middle class backgrounds because they have opportunities to access technological devices and, with internet connectivity, it enables them to be online all the time and constantly engage in online criminal activities (Holt, Navarro & Shelly, 2020: 1539). Hackers use their computer skills to gain illegal access to networks (Roos, 2012: 38). Hackers can be divided into the following three categories (Gumbi, 2018: 47):

White hat hacker - A white hat hacker is a computer security expert who has specific skills to secure systems and networks to ensure that computer security measures are upgraded and updated regularly against any intruders (Hussien, 2021:63). According to Ndaba (2013: 29), white hat hackers use their professional skills to bypass network systems for non-malicious purposes as contractual agreements with third parties to perform penetration testing and vulnerability assessment. Hussien (2021: 63) further states that it is the responsibility of white hat hackers to improve security networks that guard against vulnerabilities on the system before hackers can access networks through discovered weaknesses.

Grey hat hacker - A grey hat hacker is a computer hacker or security computer expert who occasionally finds himself/herself on the wrong side of the law with regards to ethical standards but has no malicious intent (Hussien, 2021: 63). This hacker is always online looking for weaknesses on the networks of other people without authorisation with the intent to report such weaknesses to the owners and offering to assist to upgrade the security of such owners upon payment of a nominal fee (Kempen, 2020: 1).

Black hat hacker - A black hat hacker is a cybercriminal whose intention is to cause malicious damage to the computer system for personal and financial benefits by bypassing internet security measures to exploit other people (Hussien, 2021, 64). The black hat hacker infects computer systems with viruses to steal information and destroy files. The hacker usually uses ransom-ware attacks to threaten potential victims by demanding money so that they would not release information to the public or other hackers (Kempen, 2020: 1).

2.2.1.3 Other types of cybercrime

Cybercrime is committed through computer systems and is mostly used to aid all sort of illicit acts such as financial crime and other common offences. There are different types of cybercrime such as phishing, cyber stalking, cyber bullying, cyber terrorism, identity theft and online child pornography (Mothibi & Amali, 2018: 59). The essence and characteristics of these different types of cybercrime are as follows:

Phishing - Phishing is a form of cybercrime whereby cybercriminals send fake websites to people, and it seems as if they emanate from legitimate enterprises in order to get people's personal information such as identity numbers, bank account numbers, passwords, pin codes of their bank cards and credit cards information (Grazioli & Jarvenpa, 2013: 22). It is known as online identify theft or online fraud in which the phisher solicits information via email. Phishers use internet scams to scare potential victims to comply with the contained directives and unfortunately most internet users quickly comply with those directives, completely unaware that they are being scammed (Britz, 2013: 133-134). A person could get an email that looks as if it is from the bank, asking him/her to open a link to verify his/her personal information. The purpose of sending these messages and links is to convince the receivers that responding to such invites is to their own benefit, whereas the senders want to use such information for their criminal activities (Ezeji & Olutola, 2018: 176-177). After opening the link, verifying their personal information and submitting that information through that link, the information goes straight to the cybercriminals who created that link and this enables them to defraud such people because they will have all the information that they require (Maras, 2015: 15-16).

Cyber stalking - Cyber stalking is whereby a person repeatedly sends insulting, threatening, intimidating and extortion messages to another person through emails, social networking sites, instant messages, telephone calls or any other electronic communication to harass him/her online (Siegel, 2013: 533). Maras (2015: 17) states that a person who engages in the cyber stalking may threaten or harass others to the point where they fear for their lives. Cyber stalking is an intentional harmful act by verbally harassing others via electronic communication with the intention to inflict or cause fear (Britz, 2013: 98). It is online harassment by means of sending undesired messages that could be seen as insulting, intimidating or indecent by the receiver (Mothibi & Amali, 2018: 59). The stalker could follow the victim's interactions on the internet by frequently posting threatening messages on the chat room and constantly sending annoying emails to him/her. The crime does not require any physical contact with the victim to leave psychological injuries or bruises because it happens online.

Cyber bullying - Cyber bullying involves the emotional and psychological harassment of people by teasing them, telling lies about them, making hurtful jokes on them, spreading lies about them or threatening to hurt them via electronic communication (McNeal, Kunkle & Schmeida, 2018: 17). It basically involves the exchange of condescending or contemptuous messages by one person to the other through electronic technology. The electronic devices that are often used for cyber bullying are cell phones, tablets and computers (Ezeji, 2014: 29). In most cases cyber bullying happens to children who bully each other by sending embarrassing pictures, videos, or insulting messages to harass one another electronically (Maras, 2015: 7). Mothibi and Amali (2018: 60) and Siegel (2013: 535) characterise it as a process whereby a person directs aggressive attitudes towards others with the aim of hurting or provoking them by sending hurtful text messages through information and communication technology.

Cyber terrorism - Cyber terrorism causes catastrophic damage worldwide by crippling economies and shutting down power stations through the use of computer networks. Maras (2015: 179), as well as Easttom and Taylor (2011: 210), states that cyber terrorists use computers to hack into air traffic control, causing airplanes to crash, or use bombs controlled by computers to bomb buildings. In most cases cyber terrorism is influenced by political motives or religious beliefs to sabotage the

infrastructure of the targeted country and is perpetrated through various means, such as suicide bombing, kidnappings, human trafficking, drug trafficking and raising funds for specific causes (Arquilla & Ronfeldt, 2013: 31; Britz, 2013: 90). Cassim (2012: 384) also states that cyber terrorists could use technology to commit other traditional crimes such as human trafficking, prostitution, money laundering and terrorist financing.

Identity theft - Identity theft is a form of cybercrime whereby cybercriminals use the internet to steal other people's identities, to access bank accounts and open credit accounts on their behalf (Siegel, 2013: 528). Stolen identities could be used to commit financial crimes such as buying cars, opening bank accounts, making loans and opening credit cards in victims' names (Maras, 2015: 154). The purpose of identity theft is deception and to use another person's identity to commit fraud. According to Ezeji et al. (2018: 95), terrorists and organised crime syndicates steal the identity of others to avoid law enforcement, to break immigration laws, to spy and commit other criminal activities using other people's personal information. Ezeji and Olutola (2018: 173) state that the motive of identity theft is to cause harm to the victims by using their identity for illegal activities, thus pretending that it is the victim who committed those crimes. It is a form of fraud that could be used to either defraud financial institutions or theft to obtain employment or to enter another country by means of false pretences (Britz, 2013: 117). Identity theft offenders could be people who are hiding from law enforcement for crimes they had committed, foreign nationals entering the country unlawfully, anyone who wants to remain anonymous for personal reasons or people who assist other people in any of the aforementioned considerations. According to Ezeji (2014: 21-22), some of the other techniques used by identity theft offenders are to acquire personal information of potential victims from public records, through pick-pocketing, housebreaking and social networks because most victims are not aware of the danger of exposing their personal information in the public domain.

Online child pornography - Online child pornography entails the sharing of videos and images of sexual behaviour of children online and inviting them to commit sexual self-touching online, encouraging them to watch videos of acts of masturbating videos and offenders exposing their own genitals to children online (Reddy & Minnaar, 2015:28-29).The computer or other electronic devices could be used for sharing pornographic pictures or videos to under- age children with the aim of luring them to

become victims of sexual exploitation. According to Ezeji and Olutola (2018: 173-174), access to the internet and electronic devices by children provides opportunities for sex offenders to share pornographic images with minors. The use of the internet and technology by under- age children creates a fertile ground for sex offenders to access and share sexual images of children worldwide on the internet spectrum. Sex offenders target online child pornography because it is difficult for law enforcement agencies to link potential perpetrators to this illegality because they remain anonymous. The free use of the internet by offenders and children allows them to join online forums and networks to share their interests, desires and experiences, causing children to become attracted to sexual images to lure them into sexual exploitation (Geldenhuis, 2017: 21). The free access of children to social networks is a global problem, as such children meet and chat with unknown persons for hours at a time, without the knowledge or approval of their parents and ignorant of the age gap between them and the people they are chatting to, thus making them easy targets for online child pornography (Ezeji, 2014: 23).

2.2.1.4 Malware

Malware is a malicious software programme that could be installed on other computers through emails or messages with a link without the users' knowledge. Once users open the link on the computer or mobile phone, the device gets infected with viruses (Vermaat, Sebok, Freund, Campbell & Frydenberg, 2016: 215; Schultz, 2013: 38). Malware is a malicious software programme that infects other computer programmes with viruses to destroy data, weakens their operation and compromises the confidentiality, integrity and availability of the information that the affected computers have. Stallings (2019: 487) explains that it is used to attack websites and servers of other computers through spam emails or messages. Maras (2015: 3) mentions worms, Trojan horses, spyware and botnets as some of the examples of malware that are used by cybercriminals to cause damage to computer systems or to by-pass computer operations to destroy or steal information. Ezeji and Olutolo (2018: 177) indicate that attacks on other computers come in the form of codes, scripts, content and other software. Malware presents global threats that negatively affect internet users by taking full control of the infected host and network connections to disable firewalls and installed anti- virus programmes (Rehman, Hazarika & Chetia, 2011: 69).

2.2.1.5 Sub-categories of malware

The use of technology by individuals increases the threats of attacks by malware and it compromises the security of computer systems to steal information. Malware is used by hackers and cybercriminals with the aim to attack, steal sensitive information or engage in the cybercrime activities (Holt & Bossler, 2013: 420). It exploits viruses that are transferred to the web servers secretly to infect computer systems in the web browser and to steal information through visiting the infected websites without attachments. This malware programme includes the distribution of denial of service, Trojan horse, ransomware and botnet (Holt, Burruss & Bossler, 2018: 1721). The following are some of the sub-categories of malware:

Distributed Denial of Service Attack: Distributed Denial of Service Attacks involve the disruption of the legitimate use of the computer to prevent the user from having access to websites or emails. The hacker plants the virus on the network to render the computer to malfunction, slowing down the response or making some services unavailable and block the users from accessing the network (Vermaat et al., 2016: 217). The techniques used by the attackers are to request large volumes of service from the network, thus causing the server not to respond, to be offline or overloaded and preventing it from responding to legitimate users (Ezeji & Olutola, 2018: 175). This creates confusion to the real users, trying to access the website and forces them to search the content of the web-site application thus cracking the web application to open sensitive and confidential information. The attacker then accesses the database to steal information, destroy and crash the web-site application (Minnaar, 2014: 133-134).

Trojan Horses: A Trojan horse is unlawful software used to trick computer users by making them believe that it is legitimate software and when computer users download and install the programme, it infects the computer with the virus that corrupts the network (Maras, 2015: 10-11). It looks like a legitimate programme, but it has a malicious code that is invisible. This malicious code is transferred to another computer through downloads. Tahir (2018: 21) explains that once the malicious code gets into the targeted computer, it observes the data that comes into that computer in order to steal it, delete it or corrupt it. The Trojan horse appears to be an anti-virus software that is designed to bypass the computer security measures by exploiting the user

authorisations (Stallings, 2019: 489). This programme can be inserted on the system through various ways such as being embedded in software, or email attachments that have a link or circulated to the Uniform Resource Locator (URL) that does not have a real domain name but looks like the legitimate domain name. When the user logs on to the computer and accesses a website that has Trojan horses, the data of the user such as the password stored in the computer could be copied and the updated function is deleted on the anti-viral software so that it could not to be traced back (Clough, 2010: 34).

Ransomware: Ransomware refers to the releasing of something that is held captive with payment, meaning that the computer is kidnapped (data or computer networks are blocked) and it will not be released until a ransom is paid (Willems, 2019: 89). According Minnaar, (2016) ransomware has become a cyber-threat against internet industries globally, it takes control of the computer network by encrypting data and blocking the user for using computer system unless the demand is fulfilled. When the ransom is paid out, the Crypto-Locker programme decrypts the files that are encrypted. Willems (2019: 89) further states that this scam is transported through the email with a zip attachment and once the user opens it, it plants the virus into the computer. Files of the targeted computer are encrypted, creating PDF files on the user computer screen, displaying a Crypto-Locker (software that uses various encryption methods) payment programme. This programme encourages the computer user to pay a ransom within the stipulated period for the encrypted files to be decrypted. Tahir (2018: 22) indicates that the hacker can demand the user to pay ransom but there is no guarantee that the user will be able to take back entire control of the computer and the data in it after that.

Botnet: Botnet is malicious software used by hackers to take control of a third party's computer without his/her knowledge to commit criminal activities like sending spam emails and stealing the information (Tahir, 2018: 22). The software looks for a compromised computer that is not protected by an anti-virus programme or has weak anti-virus protection and then targets it for criminal intent. The user of the computer is unaware that the device is controlled remotely by the hacker who uses botnet to attack by sending spam via email, spread viruses and denial of service attacks (Vermaat et al., 2016: 216). Botnet can also be used by cyber-gangs to steal money, identity cards,

to crack passwords and the commission of other crimes. The Core-flood malware that allows the computer to be remotely controlled is used to steal personal and financial information by observing network movements for recording unsuspecting users' every key stroke. Once the user opens the computer that is infected with Core-flood, it spreads the virus on the computer and the hacker controls the virus remotely (Siegel, 2013: 530). In other words, a botnet can be instructed by the hacker to perform certain tasks such as denial of service attacks, using another person's computer without authorisation, or making it impossible to stop the attacks because there is no point of control (Clough, 2010: 35).

2.3 CYBER SECURITY

Cyber security is the process where the government, individuals, businesses and companies ensure that security countermeasures such as security guidelines, risk management approaches, best practices and quality assurance are in place to safeguard and protect their Information Communication Technology (ICT) against cyber threats. It strives to ensure the protection of computer networks against unauthorised modification, manipulation or disruption and to give assurance to the user that the network performs its operation correctly without any harmful side effects (Stallings, 2019: 3-4). Its main purpose is to protect the country's critical infrastructure such as global submarine optic fibre networks, water plant system networks, telecommunication networks and electrical grid networks and to improve the identification of cyber incidents. It secures a reliable cyberspace that ensures citizens that their data is safe and secured (Ntsabula, 2017: 27; Du Toit et al., 2018: 117). It (cyber security) entails the protection that the organisation has to implement to safeguard online attacks, and threats to all its digital electronic platforms and the information security where data is stored, accessed, processed and transmitted for the protection of the crime against computers, sabotage and espionage. The prevention measures that can be used against cyber threats are Intrusion Protection System (IPS), pre-emptive blocks, blacklisting and cyber intelligence threats (Minnaar, 2014: 137). According to Jideani (2018: 32) cyber security risks must be identified and decisions be made on strategies that could be used to address cyber risks.

The South African Police Service is a stakeholder in cybercrime and cyber-security, as they developed cybercrime protocols to guide coordinated responses to cybercrime

incidents and interact with other cybercrime and cyber-security stakeholders to combat cybercrime (Phahlamohlaka & Hefer, 2019: 4). According to the Cybercrime Act 19 of 2020, the police have the duty to establish and maintain capacity to ensure they detect, prevent and investigate cybercrime. The South African Police Service should provide training to police officers to have skills to detect, prevent and investigate cybercrime. In conjunction with institutions of high learning they could develop and implement accredited training programmes for the police involve in combating cybercrime (Cybercrime Act 19, 2020: 78).

2.4 ENCRYPTION

Encryption is used by criminals and non-criminals to hide communication such as instant messages and emails. Caesar cipher is one of the encryption methods known in the world, its name is derived from Julius Caesar and is used to encrypt messages (Easttom & Taylor, 2011: 449). This method of encryption is to shift each letter in the message in a different direction to make it difficult for the intruder to read the communication thus encrypting messages (Jideani, 2018: 40). The main purpose of encryption is to block unauthorised people from reading the information that is stored on computer networks or mobile devices. The information is encrypted using algorithms which change the words to be unreadable on the cipher text. This encryption protects the confidentiality and integrity of information during the processing of incoming and outgoing data on networks (Hussien, 2021: 59).

The use of encryption is important to organisations, companies and government because it protects customers' and employees' personal information from fraudulent activities by securing the customers' and employees' identity numbers, credit card numbers and passwords from being stolen as result of cybercrime. The encryption protocols that are used to protect customers and employees' data stored on the computer system are Secure Sockets Layer and Secure Electronic Transaction. Secure Sockets Layer is an encryption protocol used to secure transactions that occur online to ensure that data like credit card numbers, identity numbers and passwords are protected. The purpose of using Secure Sockets Layer is to know the established link between the web server and browser to ensure that the data stored in the system is private and confidential so that transactions that occur online are protected and this method of encryption is to secure transport layers that make use of asymmetric

mechanisms and have public and private keys (Modi, 2016: NP). Secure Electronic Transaction is an encryption protocol used to protect data by using digital certificates to recognise the customer, payment gateway and merchant. This method of encryption requires customers to install cyber security software on their computer systems for protection to secure transactions that occur online against any intruder (Jideani, 2018:40-41). This could be policed through Open Source Intelligence (OSINT) in South Africa where the police can gather and analyse data that is publicly accessible online. OSINT is a cyber- threat intelligence that the police could use by browsing from the web and other crawling technology and according to Veerasamy (2017: 3), it is useful in threat alerts. This is a domain that the police can use to access information where individuals can be monitored and surveillance conducted at a broader scale (Trottier, 2015: 531).

2.5 THE PREVALENCE OF CYBERCRIME

Cybercrime in South Africa is growing at alarming rates, it is difficult to predict crime trends and impossible for the police to catch up with it because cybercrime is under-reported to police (Das & Nayak, 2013: 151). The increased use of online communication by individuals, companies, organisations and government has increased the risks of being targeted by cybercriminals who focus on stealing financial information, for business espionage and accessing government information (Kundi & Akhtar, 2014: 63). According to Dlamini and Mbambo (2019a: 2), techno-social change in the society started in the 21st century, and a moderately new phenomenon, that is cybercrime, that was unknown and un-administered by law enforcement agencies, came into existence thus leaving potential victims at the risk of victimisation and exploitation.

Cybercrime in South Africa exposes the public to high victimisation and the increase of this crime causes extensive financial loss to them. Cybercriminals use various techniques such as malicious software that is attached to the normal file and as a result it causes damage to a computer system and thereafter destroys sensitive information of government and cooperate infrastructures. Cybercriminals use other malicious software such as worms to check vulnerabilities on computers or networks to attack companies, organisations, businesses, individuals and governments as a form of assessment testing to commit cybercrime (Symantec Intelligence Reports,

2013: NP). The cybercrime that is mostly known in South Africa is E-commerce fraud where cybercriminals use the internet and computer systems to defraud victims by posting items that do not exist on the computer system deceiving victims and defrauding them of their money. Furthermore, phishing and identity theft is rising in South Africa whereby cybercriminals use emails and web pages to persuade victims to reveal their personal information and financial status to steal that information for financial benefits or use it to further other crimes. Another prevalent crime in South Africa is web hacking, whereby cybercriminals expose government, businesses and companies' websites with the aim of embarrassing and to prove computer security weakness (Ezeji, 2014: 33).

Cybercriminals use phishing scams to download malware on the computer system and distribute denial of service as a form of hacking to steal digital information that is used to commit fraudulent acts. The increasing sophistication and professionalism used online by organised cybercriminals makes it clear that government, businesses and the public are attacked by malware infections as a form of cybercrime. The cybercrime business is worth multi-billion dollars globally and is run by organised cybercriminals, employing information technology experts, professional coders and programmers that manage E-commerce sites and cloud computing service to commit criminal activities (Kader & Minnaar, 2015: 79-80). There is a huge increase in organised cybercriminals facilitated by the formation of underground online businesses where stolen goods and illegal activities are bought and sold in professional manner on the black market. The use of the dark web that is anonymous and unregulated by cybercriminals on the cyberspace to commit criminal activities makes it difficult for these criminals to be identified by police agencies across the globe (Robb, 2015: 2). The distribution of denial-of-service attacks where cybercriminals use internet and computer systems to create resistance for the computer user to use it or making the computer system not to respond is prevalent in South Africa (Ezeji, 2014: 33).

Some cyber-attacks involve intercepting information of online bankers and sending instant messages and emails to victims and deceiving them that one of their family members is hospitalised due to a car accident and money is needed for the hospital bills to be paid. This modus operandi is used by perpetrators to unsuspecting victims who could send money to them believing that the communication is genuine (Lewis,

2011: 41). Symantec Intelligence Reports (2013: NP) reveal that South Africa has the highest rates of cybercrime followed by Russia and China.

2.6 THE IMPACT OF CYBERCRIME IN POLICING

The detection and prevention of cybercrime is complex and sometimes impossible due to the borderless nature of this crime, thus posing a challenge to effective law enforcement. It is difficult for the police to detect and apprehend offenders due to the technical complexity and the fact that offenders committing this crime could be sitting thousand miles away (Kundi & Akhtar, 2014:64). Cybercrime is wreaking havoc, and it is clear that traditional methods of policing such as sector policing, community policing and partnership policing have no effect on its investigation and prevention (Reddy & Minnaar, 2015: 32-33). The investigation of cybercrime is challenging because the investigators of cybercrime often ignore, destroy, compromise and inappropriately handle digital evidence during process investigations. Although law enforcement agencies in South Africa invested in cybercrime preventive measures, they remain unprepared to use countermeasures to launch effective responses to cybercrime. They fail to utilise guiding measures that are in place in combating cyber-attacks and they find themselves under pressure to investigate, track and analyse bunch of cybercrime incidents (Kader & Minnaar, 2015: 70).

The police use delaying tactics such as not following the leads, ignoring digital evidence, destroying and compromising or inappropriately handling the investigation of cybercrime and these compromise the effectiveness of the investigation and make it difficult for them to apprehend cybercriminals. The slower the police are in detecting and responding to cyber-attacks, individuals, companies, businesses and organisations launch their own counter attacks for self-defence, which can be labelled by the police as illegal in the eye of the law or be interpreted as an illicit act of cyber vigilantism (Dlamini & Mbambo, 2019a: 6). The reluctance of the police to respond to cyber-attacks is based on their fear that they might not have enough evidence to probe the cause and progress if they react immediately. The United Nation Office on Drugs and Crime (2013: 84) states that delayed police response on cybercrime is influenced by the assumption that perpetrators can be someone looking around on the network with no intention of stealing data for criminal activities.

Cybercrime occurs in cyberspace and is technologically complex and requires the police who investigate these crimes to be technologically knowledgeable so that they could understand the nature, risks and have advance investigative approaches on cybercrime investigations (Kader & Minnaar, 2015: 71). A study conducted by the USA government indicates that there is lack of capability in the investigation of cybercrime incidents around the world, due to lack of in-house training capabilities to investigate cybercrime (US Government Accountability Office, 2014: NP). This lack of training and experience to investigate cybercrime indicates that the gathering of evidence, detection and the tracing of cybercrime suspects is difficult (Kader & Minnaar, 2015: 72). The use of traditional investigation methods is unable to deal with cybercrime because they purely focus on tangible physical evidence found on the crime scene while cybercrime incidents require cyber forensic investigation and intelligence-led investigation that focus on the evidence of sophisticated technology as well as borderless information networks (Basdeo et al., 2014: 62). The challenges in the effective policing of cybercrime in South Africa is largely as a result of the legal system and the existing laws because they are not enough as they were designed to deal with traditional crimes and not cybercrimes. Basdeo et al. (2014: 48) state that for South Africa to combat cybercrime effectively, it requires it to forge partnerships with international organisations to enable investigation, deterrence and the imposition of sanctions on cybercriminals.

2.7 THE CHALLENGES OF COMBATING CYBERCRIME

Cybercrime is a recent challenge that requires new legislation to deal with it effectively and it takes time for such a law to be developed in South Africa as it requires parliament to debate and vote on it before the president can sign it to become law. For example, it took from 1999 to 2002 (four years) for the Electronic Communications and Transactions Act 25 of 2002 to be passed into law (Eiselen, 2014: 2814). Dlamini and Mbambo (2019a: 5) state that due to the high rate of cybercrime incidents, policy makers must ensure that there is a short period between the development and the implementation of policies. Cybercrime and Related Matter Bill was first drafted in 2015, open for public comments, re-opened again for public debates in 2016 and a new draft was incorporated, which is called Cybercrime and Security Bill (B6-2017) that was submitted to South African parliament on 22 February 2017. However, Cybercrime and Security Bill delays was again due to the misunderstanding of some

terminology used, so the additional public comments were open in 2017 and the last version of the Bill was incorporated in October 2018. Therefore, Cybercrime and Security Bill was passed by parliament on 27 November 2018 but delayed again in 2019 for public comments, the Bill became law when it was passed by parliament in early 2020 and approved by the National Council of Provinces on 30 June 2020 (Minnaar, 2020: 43).

The lack of cooperation amongst government departments, companies and organisations to participate in issues regarding cybercrime is another challenge that is encountered as well as the lack of training of stakeholders who are responsible for preventing and combating cybercrime (Dlamini & Mbambo, 2019a: 5). The challenge of policing in South Africa is that the enforcement of cybercrime laws is inadequate and ineffective. Therefore, the lack of adequate law in place for cybercrime give cybercriminals freedom of operating on the cyberspace freely, without fear of law enforcement and act without any consequences (Ajayi, 2016: 9). The laws governing the South African criminal justice were developed focusing on the physical world to combat crime, and these traditional laws cannot effectively deal with electronic crimes. Basdeo et al. (2014: 62) state that crimes committed through computers are a challenge to law enforcement because they are perpetrated anywhere in the world, thus requiring the police who are well trained and experienced on forensic skills related to computer crimes. The speed in which cybercrime gets committed makes it difficult for law enforcement officials to detect, combat and prevent this crime alone. It requires partnership between academics, private sector and government departments to share intelligence and capabilities to respond to this crime efficiency and effectively. Law enforcement does not have enough resources to combat this crime alone such as sufficient cybercrime investigators, limited knowledge of computer and lack of global reach due to borderless of this crime (McMurdie, 2016: 85). The internet poses a significant challenge to law enforcement because they need to track down cybercriminals who commit crimes on the cyberspace while hiding their identities, so they need to work closely with other law enforcement agencies around the world, experienced and well-equipped personnel to gather evidence, investigate and prosecute cyber related crimes. Victims could be all over the world in different jurisdictions and the police may not have sufficient evidence required for successful prosecution (Kader & Minnaar, 2015: 73).

Koziarski and Lee (2020: 4) state that the challenge of law enforcement in combating cybercrime in domestic and international policing agencies is its ability to transcend spatial and temporal boundaries as it accesses victims via internet everywhere in the world. This trans-border crime makes it difficult to punish cybercriminals due to the fact that victims and offenders reside in different countries and prosecuting these offenders is a challenge due to different legal systems as well as lack of extradition agreements in place between countries. Other challenge is the lack of technological tools to investigate cybercrimes, insufficient training and failure to employ cyber experts to assist in combating this crime. According to Basdeo et al. (2014: 48-49), respecting other countries legal system and the principle of non-interference in the domestic affairs of other countries is an important principle of building relationships between countries and criminals in different jurisdictions use this to their advantage. The enactment and harmonisation appropriate trans-border crime procedural arrangements could play an important role in facilitating international cooperation in combating cybercrime. According to Kader and Minnaar (2015: 69) another challenge to effective policing is that victims who report cybercrime incidents do not get beneficial results because they continue to lose money as they have to embark on alternative protection mechanisms such as the institution of their own cyber-security measures.

2.8 THE PREVENTION OF CYBERCRIME

The use of Intelligence-Led Policing technologies such as the intrusion of the cyberspace for cyber surveillance helps the police to detect and monitor in-coming data and out-going data on computer networks 24/7 in order to prevent cyber-attacks. The police use these technologies for risk assessment, identification of cyber threats and content identification for the detection, investigation and the prevention of cybercrime (Widdsup, Spitter, Hylendem & Basset, 2018: 600). The use of Intelligence-Led Policing strategies plays an important role in preventing cybercrime by collecting and developing information related to cyber threats in order to eliminate them. The use of this crime prevention approach helps the police to combine problem solving, information sharing and police accountability for the prevention of cybercrime. These tactics could be used in tactical intelligence operations for imminent threats, while operational intelligence could be used to respond to the threats and strategic intelligence operation could be used for developing and implementing preventative

measures to respond to long-term threats (Thenga, 2018: 80-81). The use of cyber forensic techniques in policing can help to infiltrate cyber-attacks wherever they take place and cyber forensic could use computers for counter attacks through deflection, disruption or inflection (Widdsup et al., 2018: 600).

The South African Police Service developed and enhanced cyber intelligence and cyber security in order to predict cyber -related threats to deter criminals from committing cybercrime. Other cybercrime prevention approaches used in policing are initiating cybercrime training for police officers at station level for them to acquire basic cybercrime skills and enabling them to understand how to identify, categorise and open dockets of cybercrime offences (Ezeji et al., 2018: 108). Training will enable them to obtain evidence from electronic devices and internet networks because they have experience and knowledge to collect this fragile evidence. It will enable them to handle this evidence with caution, retrieve it with care and preserve it properly (Ezeji, 2014: 112). South Africans also take part in cybercrime prevention by blocking the paths used by cybercriminals by placing obstacles (installing anti-viruses, firewalls and using strong passwords) to prevent them from successfully committing cybercrime and limiting the lucrative nature of cybercrime. Internet users also prevent cybercrime by applying cyber-security measures on their personal devices as first step, not replying to unknown emails and to report spam emails to police immediately (Du Toit et al., 2018: 116). The involvement of businesses, organisations, companies and government departments to act collectively against cybercrime and to report crime to police helps in apprehending, convicting and sentencing cybercriminals. The police work together with the community to forge partnerships in preventing cybercrime to restore trust so that communities can be motivated to report cybercrime to police freely and without becoming scape goats after reporting cybercrime (Ezeji et al., 2018: 102).

The police can use education and awareness campaigns to empower the public to prevent cybercrime by being knowledgeable about the most common hacking tactics (for example phishing, social engineering, packet and sniffing etc.) to safeguard their personal information in cyberspace (Herhalt, 2011: NP). This warrants the use of local laws, together with international laws for cooperation and coordination with global cybercrime enforcement agencies and courts to form international treaties on cybercrime in helping to prevent it (Kundi & Akhtar, 2014: 68). The police can prevent

cybercrime through detecting cyber incidents, verifying the incidents and collecting volatile evidence. This should be based on known facts so that a back-up system could be created and investigation conducted to identify who committed the crime and how the incidents occurred for the police to be able to isolate and contain offender systems. The police must regularly observe networks to monitor attacks, future attacks, and to ensure that the system is in its original state with cyber-security measures, and then document the responses with remedies taken, review responses to adjust accordingly (Kader & Minnaar, 2015: 75).

2.9 CONCLUSION

The use of the computer technology presents challenges to law enforcement agencies around the world as it increases the occurrences of transactional crime, as these types of crime can take place everywhere. The law that is used in many countries to address crime focuses only on traditional crime and this law is inadequate to deal with cyberspace crimes that have no geographical or territorial boundaries because computer systems can be easily accessed everywhere in the world to commit cybercrime. The investigation, detection and prevention of this crime are difficult because of the absence of accurate data that shows the number of cybercrimes that go undetected and unreported to law enforcement agencies.

South Africa has pieces of legislation and guidelines that are used to address cybercrime but there is ample room for improvement to have harsher penalties for offenders, tighter cyber-security measures, by encouraging cybercrime awareness campaigns for the public and training to law enforcement agencies to be knowledgeable on cybercrime. An effective fight against cybercrime also requires partnerships with international communities to expand the jurisdiction to other countries to allow them to prosecute any person who commits cybercrime, whether within those countries or outside them and to encourage extradition of any person who flees to the home country to avoid sanctions.

CHAPTER THREE: THE USE OF INTELLIGENCE-LED POLICING TO COMBAT CYBERCRIMES IN SOUTH AFRICA

3.1 INTRODUCTION

Cybercrimes present problems that negatively affect the quality of life of millions of people around the world and impact the economic growth and development of countries negatively. They pose challenges to the policing fraternity globally in the detection, prevention, control and management of cybercrime threats (Matsaung, 2019: 43). The use of electronic devices (technology) has increasingly made the digitalisation of information available at lower cost and also increases the activities of cybercriminals (Gemke, Den Hengst, Van Rosmalen & De Boer, 2021: 190). Cybercrime is a serious concern in South Africa like in many other countries, because it is increasing at an alarming rate and it is very difficult for the police to combat. Cyber-security experts believe that to combat cybercrime effectively, police officers require specialized training, knowledge and skills. The community and business at large are of the opinion that the surge of cybercrime is out of control and that the police are not coping. Therefore, the situation compels the community and businesses to provide their own protection by employing cyber-security measures against cybercrime (Govender, 2012: 79).

The policing fraternity around the world must refrain from using reactive policing model styles such as community policing, partnership policing and sector policing which are not coping to deal with cybercrimes, and rather employ proactive smart policing model such as Intelligence-Led Policing to combat cybercrimes. Intelligence-Led Policing could enable the police to develop strategies that can be used to detect, disrupt and prevent cybercrime before it can occur. This could help the police to produce sophisticated technology and software to help in understanding the series, linkages and patterns of cybercrimes. Such strategies would help the police to perform in-depth analyses, identify cyber threats and evaluate the results in solving cybercrime. The use of this crime prevention approach in policing can help in strategic decision-making to support innovation and data collection as the best model to deal with cybercrime (Budhram, 2016: 80). This policing model guides the police to be more strategic, future- oriented and more focused in combating cybercrime. Intelligence-Led Policing is a business model for policing and it can be used to collect, analyse and evaluate

crime information to produce actionable intelligence. That can then be used as operational, tactical and strategic intelligence to investigate, prevent, reduce and disrupt cybercrime (Gibbs, McGarell & Sullivan, 2015: 244).

Intelligence-Led Policing is an application of crime intelligence analysis as decision making tool on the threats of crime in societies for the prevention and reduction of cybercrime by using police operational activities and intelligence communities as evidential base. The role of this model in policing is to ensure that intelligence officers and crime analysts are at the frontline of police operations to use police resources more efficiently to help in the prevention, investigation and prosecution of cybercrime (Mugari, Maunga & Chigariro, 2015:88). It is therefore imperative to have a model based on the collection of intelligence to analyse it to become evidence that can be used to develop strategic and tactical responses to combat cybercrime across law enforcement agencies. Carter and Fox (2018: 3) state that smarter modern policing is the best in capitalizing raw crime information inputs in both qualitative and quantitative analyses to alert the police in monitoring, detection and prevention when targeting prolific offenders of cybercrimes.

3.2 THE VALUE OF CRIME INTELLIGENCE IN COMBATING CYBERCRIME

The South African Police Service (SAPS) has a division of crime intelligence and its role is to track down criminal elements within the country. The role of crime intelligence in policing is the collection, analysis and interpretation of crime data from known sources, informers and undercover agents to support the police during their operations in combating crime (Scheepers & Schultz, 2019: 2). According to the National Strategic Intelligence Act of 1994, crime intelligence gathers intelligence in such a way that the collection, correlation, analysis, dissemination and results can produce outputs that can be used in the prevention, reduction and investigation of crime. This will also include cybercrime where they should share crime data to identify, understand and explain crime trends to address the problem. According to Ezeji (2017: 188), the crime intelligence division within the SAPS has the responsibility to make electronic interception, wiretapping, surveillance counter measures and covert tracking for the purpose of combating cybercrime.

Mashiloane (2014: 49) states that they (crime intelligence) have to ensure that crime information is gathered, correlated, analysed, interpreted and disseminated to support the mandate of the SAPS as outlined in section 205(3) of the Constitution of the Republic of South Africa of 1996. Their duty is to incorporate investigation and prevention into one crime funnel to predict future crimes, deploying effective ways to profile criminals and target their business enterprises (Mugari et al., 2015: 87). The daily duties of police officers differ from those of crime intelligence officers because police officers maintain law and order in society by reducing, preventing, arresting and investigating crimes; whereas crime intelligence officers conduct in-depth search of any kind of crime information for collection, analysis, interpretation and verification to convert that collected information into actionable intelligence for risk assessment and cyber threats prevention (Budhram, 2016:81).

It is important to note that the role of crime intelligence is not only to collect information about criminal activities but also to verify the correctness of the collected information. Converting that information into actionable intelligence helps the police in planning daily operational activities and police executives to devise strategies that can help in preventing and investigating crime incidents (Van Graan & Zinn, 2015: 42). Matsaung (2019: 56) emphasises that crime intelligence should be able to trace criminal gangs, identify them, know their associations and their intentions, and formulate suitable interventions to prevent such activities.

3.3 THE USE OF INTELLIGENCE TO COMBAT CYBERCRIME

Intelligence is a raw material product of crime intelligence and may be used by police as end results for preventing and investigating cybercrime. Mashiloane (2014: 53) states that it (intelligence) can also be used for identification, apprehension and prosecution of cybercriminals. It is information collected about criminality that should be processed to form intelligence for tracing and combating crime. The aim is to share information that is accurate and to compile it into actionable intelligence that can be used to combat cybercrime. Such intelligence must be systematic, scientific and shared accurately so that it can be disseminated in the right direction to those people who use it to prevent crime threats (Mugari et al., 2015: 89). It renders for the collection of crime data that can be used by the police to target cybercriminals and understand the context of criminality so that cyber threats, offenders and business enterprises can

be identified and dealt with. Bureau Justice Assistance (2014: 4) highlights that the collection of data requires planning so that crime analysts will be able to collect, analyse and verify information to identify the threats before it is disseminated to crime prevention and investigating officers for it to aid in the arrest of offenders and to prevent further crimes.

Budhram (2016: 82) states that intelligence is a report on the information that is collected from various sources about criminality that focuses on the behaviour of offenders such as the identity of offenders, their modus operandi, as well as series and trends of crime threats. On the other hand, Intelligence-Led Policing is a managerial philosophy of law enforcement agencies worldwide that employs intelligence at the forefront of decision making. It seeks to move from reactive policing to proactive policing of crime prevention that involves a shift away from responding to a few crime threats in isolation to more future-orientated and strategic management of criminal activities (Burcher & Whelan, 2019: 139-140). It positions intelligence at the forefront of decision making in crime prevention and crime control measures (Ratcliffe, 2016: 89). The police use intelligence as the foundation for defining priorities and strategic and police operational work activities in the prevention and suppression of cybercrime. It involves making proper decisions on police activities, actions, the use of available human resources and the allocation of material as well as technical resources (Fick, 2019: 30). Intelligence-Led Policing leverages intelligence gains by using multiple sources such as surveillance, informants and other law enforcement agencies to target cybercriminals. The purpose of this proactive policing philosophy is to identify crime incidents, know where the target come from, trace the offenders and prevent attacks (Carter & Fox, 2018:4-5). Ezeji (2017: 289) further elaborates that the use of Intelligence-Led Policing in combating cybercrime is a collaborative effort in improving intelligence operations and solving cyber threat problems to help law enforcement agencies to respond effectively in solving crime. According to Baker (2012:8), the police require intelligence to understand the picture of crime, the nature and extent of the problem, the trends and where main threats are accurately; and to also adopt Intelligence-Led Policing strategies to enhance effective crime reduction and prevention measures.

3.4 THE INTELLIGENCE-LED POLICING CONCEPT

The concept “Intelligence-Led Policing” is vague and lacks a uniform definition which may be the reason why many law enforcement agencies find it difficult to comprehend it fully and implement it holistically. To understand Intelligence-Led Policing better, the use of data, information, knowledge and intelligence principle, the consecutive steps such as data, information, knowledge and intelligence are placed in hierarchical order (Gemke et al., 2019: 191). Data involve the collection of facts about the events; if meaning is added it becomes information and knowledge is richer than data or information, as it provides broader and deeper information about the context, meaning and interpretation (Davenport & Prusak, 1998: NP). Intelligence incorporates the accumulation of data, information and knowledge that is generated mostly through Intelligence-Led Policing. According to Gemke, et al., (2019: 191), Intelligence-Led Policing uses proactive actions to anticipate and predict crime and security threats so that the police can use end results to reduce risk, harm and to prevent crime.

Intelligence serves as a decision-making tool on police strategies to reduce and prevent cybercrime with the support of other law enforcement agencies and stakeholders. Budhram (2016: 81) explains that Intelligence-Led Policing is a unique model that provides managerial guidance to the police in crime reduction, crime prevention and disruption that is pivotal to strategic management and effective policing in targeting criminals. It is seen as the vehicle that places crime intelligence at the forefront in the decision making by law enforcement agencies (Burcher & Whelan, 2019: 139). It helps to achieve police objectives by managing both criminal intelligence and planned operational police work that can be used to prioritise, strategize and operationalise police resources in the prevention, suppression and elimination of security threats. Fick (2019: 30) states that Intelligence-Led Policing helps the police to make informed decisions on their activities and the utilisation of material and technical resources. It should take the lead in crafting operational strategies that are designed to deal with criminal activities. This means that the police should always be ahead of criminals on physical and technological innovations in order to deal with crime challenges effectively (Mugari et al., 2015: 89).

Intelligence-Led Policing enables the police to collect, analyse, interpret, verify and disseminate cybercrime information and activities. It forms part of the solution in

response to threats or risks of emerging and changing crime threats (Carter, 2016: 438). It targets prolific and serious offenders by using available resources on operational, tactical and strategic levels in the investigation of committed crimes (Ezeji & Olutola, 2018: 169). Finally, it assists the police to identify criminals, understand their intentions and to intervene by apprehending them. According to Matsaung (2019: 56), this stems from the fact that the police deal with evidence gathering, problem solving, information sharing and police accountability.

3.5 THE EVOLUTION OF INTELLIGENCE-LED POLICING

Intelligence-Led Policing as a business model of policing was implemented in the first decade of the 21st century to deal with various transactional crimes and it has been the latest model of crime prevention model used countrywide in combating crime in the United Kingdom (Gibbs et al., 2015: 244). Govender (2012: 83) emphasises that Intelligence-Led Policing, also known as Intelligence-Driven Policing came into being when there was violent crime in the United Kingdom and traditional crime prevention approaches were failing to cope with the rapid changes in globalisation and increased opportunities for transactional organised crime. According to Burcher and Whelan (2019:140), the National Intelligence Model is a business model of policing that introduced Intelligence-Led Policing and it was used by policing agencies around the world. This model has been adopted in many countries around the world such as the United States, Canada, Australia and New Zealand. The reason for adopting this model in the United Kingdom was because the police took too long to respond to offences and could not address the problem of repeat offenders (Budhram, 2016: 84). The reports that were published in 1993 by Audit Commission and Her Majesty's Inspectorate of Constabulary indicated the need to use intelligence, surveillance and informants in tackling the problem of repeat offenders for the police to combat crime (Budhram, 2016:84-85). The Intelligence-Led Policing model changed policing styles from a reactive policing practice approach to a proactive approach, placing the police in a position to manage, prevent and control crime. Traditional law enforcement practice to prevent crime focuses on the social control associated with crime, which is ineffective to deal with huge crimes, whereas Intelligence-Led Policing moves towards risk management to deal effectively and smarter with crime (Budhram, 2016: 85).

Burcher and Whelan (2019:140) state that the use of Intelligence-Led Policing gained momentum after the terrorist attack in the United States of America on 11 September 2001 and many countries decided to examine the UK National Intelligence Model to use intelligence to combat crime. The United States launched an Intelligence Sharing Summit in March 2002 that was aimed at creating a Global Intelligence Group to develop a criminal intelligence sharing plan under the command of the Investigative Operations Committee of the International Association of Chiefs of Police. According to Mugari et al. (2015: 88), some of the aims of the criminal intelligence sharing plan is to ensure that it promotes Intelligence-Led Policing, build intelligence system and intelligence process principles and policies. The plan is to ensure that law enforcement agencies around the world have strategies to gather, evaluate and disseminate intelligence so that it protects individuals' right of privacy and on the other hand to combat transactional crime, organised crime and public disorder.

The South African Police Service introduced the Intelligence-Led Policing in 1995 due to the many organised crime syndicates (Govender, 2012: 83). It used it to gather intelligence through conducting network operations and undercover or covert projects dealing with informers, agents and electronic surveillance. Intelligence analysts use undercover operations for recruiting informers or agents to target organised crime syndicates and network operations and analyse crime to support police with crime detection, crime prevention and crime investigation (Van Graan & Zinn, 2015: 44-45). Intelligence-Led Policing to combat organised crime syndicates was used to identify crime, and once a crime was detected through reports or the police's own discoveries. Crime analysts would start collecting information such as the location of crime, identity of suspects, victims and witnesses, using among others the modus operandi of crime through the information harvested from dockets. They relied on intelligence harvested from sources such as previously arrested suspects, as well as their associations and structures. Mashiloane (2014: 230) states that overt and covert techniques are used to collect information through linkage analysis charts or association network analysis charts to identify suspects, crime activities and business enterprises. Association network analysis charts are used as the results to assist investigators to trace money or paper trails in organised investigations.

3.6 THE CHALLENGES ON THE USE OF INTELLIGENCE-LED POLICING TO COMBAT CYBERCRIME

Intelligence-Led Policing is implemented by law enforcement agencies around the world as the latest modern policing approach to deal with crime. Its challenges revolve around the substantive ambiguity of the conceptual foundation and that it has not yet been seen as an effective approach in dealing with cybercrime (Carter & Fox, 2018: 2). According to Darroch and Mazerolle (2013: NP), the use of this approach is seen by the police as bedevilling crime information, lacking interoperability, not having mechanisms for reporting and recording intelligence, as well as creating silos and duplication in the collection of crime information. The lack of leadership in the implementation of Intelligence-Led Policing from the foundation phase is an innovation struggle (Burcher & Whelan, 2019: 141). The police are unable to use Intelligence-Led Policing to combat cybercrime because there is no evidence that support the notion that the use of Intelligence-Led Policing can help in combating cybercrime (Jensen, Regens & Griffin, 2013: NP). The lack of resources and training amongst law enforcement agencies is a challenge in the implementation of this model (Cichoracki, 2020: 6). This aspect is coupled by the failure of police management to clarify the value of this model in policing where it is implemented, rather than labelling it as subterfuge - a clandestine and covert activity conducted by police as illegal in the name of intelligence and including the degree of moral ambiguity. Ezeji (2017: 167-168) claims that the resistance by leaders to use this model is due to lack of training as they only have the background of a reactive police approach rather than also having a background of disciplines such as criminology and forensic investigation. Another challenge to full implementation of this model is the political agenda whereby the executive resists the use of this innovative model to deal with crime and prefers to rather use a reactive police style which is ineffective (Goldstein, 2003: 7).

Mashiloane (2014: 170) emphasises that the use of Intelligence-Led Policing is traced back to the 1990s in UK as an innovative way to combat technological crimes, but surprisingly it had not been used to combat cybercrime by law enforcement agencies around the world. Cichoracki (2020: 8) supports this by stating that the use of this effective model of policing in serious crimes and terrorism other than in cybercrime reflects the bias of policing. The paucity of information on cybercrime in policing results in law enforcement agencies still employing a reactive approach which is not

necessarily very successful. According to Zinn (2011: 11) there is lack of research data on Intelligence-Led Policing as well as public scrutiny research on Intelligence-Led Policing in South Africa.

It is important for law enforcement agencies to understand that implementing an Intelligence-Led Policing approach is a positive shift and it can bring proactive information to respond to crime. The application of Intelligence-Led Policing is a worthy adoption and needs to be implemented (Ezeji, 2017: 167-168). The success of Intelligence-Led Policing commands unity from the organisation, as well as cultural changes and police leadership should provide leadership, ownership and understanding of the value of Intelligence-Led Policing in cybercrime prevention. Maintaining partnerships between the police, community and external stakeholders gives assurance and emphasises the need for adopting Intelligence-Led Policing to help in problem solving and effective cybercrime prevention strategy (Ratcliffe, 2016:192).

3.7 THE USE OF INTELLIGENCE-LED POLICING IN COMBATING CYBERCRIME

The police use an Intelligence-Led Policing approach for the collection and analysis of information to render it a usable intelligence that should inform their operational, tactical and strategic decisions on combating cybercrime. This crime prevention approach underpins aspects of policing such as partnership policing, neighbourhood policing, sector policing, community-oriented policing as well as problem-oriented policing to prevent and investigate serious crime, organised crime, terrorism and cybercrime (Buckley, 2014: 32). It is a policing business model to reduce harm, prevent and disrupt crime, and it pays attention to crime hot spots, offenders and victims for it to be used by the police to make appropriate decisions in combating crime (Ratcliffe, 2016: 65). Intelligence-Led Policing relies on the ability to collect and analyse information to solve problems and make decisions on cyber threats with the purpose of solving crime problems and relying on proactive information sharing with other law enforcement agencies to identify crime threats (Bureau of Justice Assistance, 2014: 2). Intelligence-Led Policing combines problem solving policing techniques, sharing information amongst law enforcement officers and promotes accountability on the police leadership through intelligence operations. It promotes the use of collection, analysis and dissemination of crime data to understand the situation

that contributes to the causes of crime and police action to use actionable intelligence products as responses to target crime threats and future changing threats (Mugari et al., 2015: 88). The above could also be used for the prevention, combating and investigation of cybercrime.

Intelligence-Led Policing could be used to identify, examine, prevent and respond to cybercrime and its threats. It has the capability to collect large quantities of data, examine it and interpret it so that the police are able to use it to understand crime patterns, identify individuals, their businesses and the location of crime within communities. Ronczkowski (2012:115) states that it could help the police to monitor their performance on responding to crime, monitoring the shift of crime threats and ascertain that changes are implemented. It is important to note that the police use Intelligence-Led Policing as data management and collection of information into evidence-based intelligence so that collection and analysis of intelligence can be central to contemporary policing, which should include the policing of cybercrime. It makes it easy for the police to profile offenders, map crime, link offenders and predict the next move of individuals and groups. Disruption and deterrence are part and parcel of Intelligence-Led Policing, with the aim of supporting management by acting as preventing and investigating tool to form an integrated crime and criminal analysis command structure (Ezeji & Olutola, 2018: 169). Carter (2016: 439) believes that it is seen by scholars and policing experts as a component of police strategic leadership to integrate robust analytical techniques, evidence-based practice and crime prevention goals. It has the capability of dealing with serious crime, including cybercrime, human trafficking, drug trafficking and terrorism which are trans-border crimes, and it is effective in terms of searching the best evidence in combating crime other than following a reactive police style that relies on suspects' confessions and surveillance in combating crime. According to Budhram (2016: 85), it is viewed as a crime management philosophy, concentrating on incorporating crime into one funnel by using proactive investigation techniques, forensic science methodology and apprehending offenders.

The role of Intelligence-Led Policing is to ensure that police work smarter on all crime, including cybercrime in the prevention of, and addressing the crime threats within communities. The aim of Intelligence-Led Policing is not to re-imagine the role of the

police in crime prevention, but to emphasise that the police re-imagine working smarter to the application of their own authority and capacity to deal with crime (Carter & Fox, 2018: 6-7). The use of this model of policing is shown as a top-down managerial philosophy which uses intelligence for risk assessment, threat analysis and crime management. Cowan, Burton and Moreto (2018:NP) state that Intelligence-Led Policing enables analysts to use its applications as strategies to collect, analyse, interpret, evaluate and disseminate crime data that can be used within and outside the organisation in contrast to traditional policing strategies. It could be utilised for operational purposes by crime analysts to reduce cybercrime and ensure that they use these crime reduction tactics to focus on preventing cybercrime related activities. This is done through an in-depth analysis of gathering information from various sources such as informants, crime reports and offenders, as well as using witnesses and the surveillance of suspects (Zinn, 2010: 27). It could be used to target cybercrime offenders for further investigation and establishing links with other crime and connections with other criminals. The police use surveillance and informants to identify criminals in order to know where they live so that they can make informed decisions on operational, tactical and strategic intelligence based on accurate information that will be actionable intelligence that could direct the police to the geographical areas of cybercriminals (Bureau of Justice Assistance, 2014: 34). This could not be used in its current format for cybercrime and will have to be adapted to deal with crimes in cyberspace.

3.8 THE VALUE OF USING INTELLIGENCE-LED POLICING IN PREVENTING CYBERCRIME

The value of using Intelligence-Led Policing relies on gathering intelligence and using it on cybercrime and crime prevention strategies to bolster the effectiveness and efficiency of police operations. The police use control strategies under the control of the station commander who is responsible to set priorities that focus on identifying criminals, hot spots and use intelligence-led investigation to link series of crime (Ratcliffe, 2016:64-65). Decision making is the product of Intelligence-Led Policing whereby top-down managers provide leadership to the uniform and traffic officers as well as detectives, and provide guidelines on how resources should be deployed. Intelligence-Led Policing therefore focuses on the core business of policing, dealing with the identification of cybercrime trends, cybercriminals and developing operational

response mechanisms to deal with them. The Bureau of Justice Assistance (2014: 10) affirms that Intelligence-Led Policing is aggressive in gathering intelligence and processing it to be actionable intelligence that could be shared with law enforcement officers for use in their planning and operations.

The researcher is of the view that Intelligence-Led Policing can be used to combat cybercrime. If they do not employ it, police will find themselves playing a game of catch-up and there will be no targeted deployment of resources because the police will be unaware of the cyber risks that need to be addressed. The police will not be able to develop a cybercrime prevention strategy that is guided by intelligence gathering and analysis. Fick (2019:31) states that, Intelligence-Led Policing is recognised by law enforcement agencies as the most important innovation of the 21st century to trace, detect, investigate and prevent cyber related crimes. This renders Intelligence-Led Policing the lifeblood of modern policing that enables the police to identify cyber-attacks that are active in cyberspace and which can be linked to other cyber related crimes that are likely to occur (Buckley, 2014: 46). It is able to collect and analyse crime information to understand the occurrence of criminal acts, consequently enabling the police to develop tactical and strategic responses that can be used for dealing with such acts (Carter, 2013: 27). According to Budhram (2016: 86), the police use Intelligence-Led Policing by means of overt and covert actions to target cybercriminals through managing online crime and setting traps on cybercrime hotspots to investigate cyber-attack related incidents and installing cybercrime prevention measures to tackle cyber threats.

Intelligence-Led Policing gathers data and intelligence from various communities, law enforcement agencies and undercover agents more efficiently and effectively to ensure that police resources are deployed to address crime and crime threats (Carter & Fox, 2018: 7). The use of the outcome of intelligence is fundamental in crime prevention because it leads to intelligence tactics for disruption, prevention and reduction of cybercrime. Van Graan and Zinn (2015: 44) indicate that the objectives of Intelligence-Led Policing are to focus on crime intervention and disruption to tackle crime threat incidents using the intelligence as the basis of decision making and intervention strategies. Based on the fact that Intelligence-Led Policing could collect, analyse, coordinate and disseminate crime data, that intelligence could be applied for the prevention of cybercrime and dealing with cyber threats, therefore making it

possible for intelligence to be used operationally, tactically and strategically to deal with crime threats (Budhram, 2016: 89). It could be the vehicle that drives crime prevention strategies through the identification of cybercrime incidents, cybercrime analysis, tracing of cybercriminals and targeting future cyber-attacks. According to Ezeji (2017:208), the role of this crime prevention approach supports operational, tactical and strategic tasking to tackle crime threats because complete and reliable crime data produce actionable intelligence that could be used for crime prevention and disruption.

3.9 THE USE OF INTELLIGENCE-LED POLICING AS CYBERCRIME REDUCTION, CRIME CONTROL AND DISRUPTION

The principle of Intelligence-Led Policing is to build deterrence and availability of police presence in crime environments, with the aim of targeting environments where there are higher rates of crime and to forge partnerships with other law enforcement agencies, non-government organisations and communities to prevent crime (Mashiloane, 2014: 180). Intelligence-Led Policing is a police business model that focuses on the analysis and intelligence prioritising of crime hot spots, victims, prolific offenders and criminal groups. It facilitates crime reduction, control and disruption by means of strategic and tactical management to deal with related crimes (Ratcliffe, 2016: 141).

3.9.1 The use of Intelligence-Led Policing to Deal with Cybercrime Reduction

Crime reduction requires the police to be cognisant of available resources and is an action that provides net benefit after considering the impact of displacement and diffusion of benefits, fear of crime and impact from other prevention programmes that may be attributed to any specific crime reduction activities (Ratcliffe 2016: 132). Cybercrime reduction seems to be most important approach that can be used in policing to fight cybercrime because it focuses on cost effectiveness. The use of Intelligence-Led Policing in cybercrime reduction can pool resources with other law enforcement agencies that have the direct capacity to deal with cybercrime. Ezeji (2017:247) opines that the police use tactical strategies, coupled with problem solving and preventative tactics in the most effective ways for crime reduction. He further believes that the use of problem solving is not intended for street crimes only, as originally, problem-oriented policing was intended for terrorism, human trafficking,

drug trafficking and online crimes. According to Ratcliffe (2016:142), once the police use their knowledge and resources, they can influence other agencies that combat crime and vicariously impact on criminal activities, broadening the possibilities of crime reduction, thus moving from Intelligence-Led Policing to a more inclusive crime control model.

3.9.2 The use of Intelligence-Led Policing to Deal with Cybercrime Control

Crime control is the management of the criminal activities that have already been committed to ensure that they do not spiral out of control. Cybercrime prevention is key in dealing with the cybercrime control approach for identification, arresting and prosecuting criminals. It entails long-term cybercrime control whereby the prevention can help police improve their ability to bring cybercriminals to justice. Intelligence-led crime control can assist in reducing many crime -related offences from which the police can demonstrate competence for crime control (Ezeji, 2017: 251). According to Ratcliffe (2016: 133), crime control focuses firstly on identifying where the attacks come from, secondly, reducing the risk associated with crime and thirdly, to intervene to prevent future crime by arresting and prosecuting criminals. This is also applicable as cybercrime control measures. Ezeji (2017: 249) indicates that intelligence-led crime control relies on adequate investment in measuring and monitoring crime in cyberspace to ensure open access to crime and justice information for the evidence to develop policies that are flexible and an eclectic approach to control criminal activities. Intelligence-Led Policing is a business model in policing that allows police commanders to interpret crime environments more carefully to understand cybercrime more comprehensively to make informed decisions in responding to cybercrime challenges.

3.9.3 The use of Intelligence-Led Policing to Deal with Disruption of Cybercrime

According to Ezeji (2017:250), Intelligence-Led Policing can be used to disrupt the business operation of cybercriminals for a certain period through certain police actions. Disruption is any process taken for inhibiting a threat of crime through law enforcement and regulatory actions that disturb the normal and effective business operation of criminals (Gills, 2013: 317). Ratcliffe (2016: 132) describes such disruption as any tactics used by the police to block criminal from committing crime. Levi and Maquire (2012:10) indicate that disruption removes police activity from judicial oversight,

meaning that there are possibilities of potential abuse, and therefore organisations that employ disruption activities should have supervision and monitoring structures to ensure that disruption takes place within legal frameworks. Ezeji (2017: 251) explains that disruption and deterrence sit at the heart of Intelligence-Led Policing. From an Intelligence-Led Policing perspective the three levels of cybercrime prevention are: first prevention level which requires decision makers to identify the systemic weakness that offenders exploit so that strategic cybercrime problems can be resolved urgently; the second cybercrime prevention level requires decision makers to prioritise resource allocation and targeting; while the third cybercrime prevention level requires prevention benefits to succeed from the arrest and prosecution of cybercriminals.

3.10 THE ANALYTICAL TECHNIQUES FOR INTELLIGENCE-LED POLICING TO COMBAT CYBERCRIME

Analytical techniques include a range of skills possessed by crime analysts such as trend identification, hot spot analysis, network analysis, operational intelligence assessment and results analysis as effective law enforcement activities for crime reduction initiatives and investigation approach (Ratcliffe, 2016: 97-98). According to Cornish (2011: 133), analytical techniques can be used to identify ways in which crime can be disrupted and determine the procedural sequences of crime when it occurs. Townsley, Mann and Garrett (2012: NP) assert that Intelligence-Led Policing constitutes an analytical technique that assists crime analysts to understand the entire picture of crime as evidence-based approach and to guide them in the data collection, data interpretation and data verification to establish the process of combining data to infer the cause of crime and advance to a more insightful analysis. Ratcliffe (2016: 99) further points out that analytical techniques that are relevant to Intelligence-Led Policing interpret the criminal environment and influence the decision-maker to think meaningfully, emphasising that the analytical techniques that are relevant to Intelligence-Led Policing are crime mapping and spatial analysis, structured thinking, crime scripts and hypothesis testing.

3.10.1 The use of Crime Mapping and Spatial Analysis to Understand Cybercrime

Crime mapping and spatial analysis are central to analytical techniques for the police to deal with cybercrime and are essential tools of criminological research as statistical

analysis to conduct trends of cyber related crimes (Clark, 2004: 60). Ratcliffe (2016: 99) affirms that the use of crime mapping and spatial analysis can help the police to understand the links between specific crime theories that are instrumental to divulge knowledge about crime hotspots, specifically on routine theory, crime pattern theory and the rational choice theory. These theories are collectively known as opportunity theories and recognize crime areas and people within those areas (Ezeji, 2017: 215). This view is supported by Matsuang (2019: 34) who states that environmental criminology looks for crime patterns and explains the environmental influences that can be used by crime analysts to arrive at rules that enable the prediction of the emerging crime problems as design strategies to inform development that can be used to prevent crime.

Environmental criminology focuses on the notion that the use of the electronic devices creates opportunities for offenders to commit cyber- related crimes and people often use their electronic devices via the internet without protection (Santos, 2013: 26). The use of automated and online mapping systems in policing can help in concentrating cyber- related crime or recent incidents. According to Ratcliffe (2016: 100), crime analysts should use crime mapping and spatial analysis as useful jumping-off points for a deeper inquiry rather than the final junction. Environmental criminology focuses on situational crime prevention and repeated victimisation in cybercrime. These theories explain criminal activities in detail, such as where and why offenders target certain people, where those offenders reside, their places of work and studying (Wartell & Gallagher, 2012: NP).

3.10.2 The use of Structured Thinking to Understand Cybercrime

Structured thinking techniques are an analytical tool for strategic intelligence analysts and comprise various useful skills that help to focus police officers who are struggling with complex crime problems (Ratcliffe, 2016:100). Ezeji (2016: 215) explains that analytical tools enable collaborative thinking about difficult strategic problems on how the police could deal with complex crime. Conversely, structured thinking deals with different skills employed by crime analysts as a set of tools that most analysts use in tactical and operational work to combat crime (Heuer, 2009: 10). Structured thinking is seen as techniques that assist the police's long-term view picture of crime and enhance strategic planning in policing (Ratcliffe, 2016: 100). According to Ezeji (2017:

215), structured thinking techniques can help in investigating data and aggregating one case to another as well as helping in discovering new crime patterns that may lead to the investigation and prevention of crime. These analytical tactics require analysts to have the knowledge of qualitative techniques such as competing hypothesis, force-field analysis, Delphi analysis and scenario generation. Ezeji (2017: 215) adds that they help to share common crime incidents and group them into one crime funnel so that they can break down a crime problem into one manageable analytical chunk.

Ratcliffe (2016: 100) indicates that analytical tactics can help to identify what the characteristics of crime incidents in a neighbourhood are, as well as when crimes are committed in specific regions and what factors cause crime in those regions. Such tactics indicate factors such as how the police can deploy their resources to address crime; how people can protect themselves against crime-attacks; who are often the victims of crime; and how best to protect the victims. Ezeji (2017:216) elaborates that for a more insightful and structured approach for crime analysts and the police to succeed, an identifiable decision-making system to support the application of the results in both intelligence system and decision system is required. Flood and Gasper (2009: NP) argue that structured thinking seeks to mitigate cybercrime risks. Ratcliffe (2016: 101) supports this by stating that structured thinking becomes the mainstream analytical process of Intelligence-Led Policing, as it helps police to address more pernicious and thorny crime attacks that they face and to identify cybercrime barriers.

3.10.3 The use of Crime Scripts to Understand Cybercrime

Crime script is a process that describes an action of event or accident in sequence (Ezeji, 2017: 216). It aids crime analysts to understand structured thinking about the cybercrime problem. The idea of crime script comes from cognitive psychology, and it helps crime analysts to understand the stage of cybercrime such as locations of the attackers, offenders and to identify electronic device used to attack. Crime scripts can be used in various crimes, specifically in the organised crime and more complex criminal activities such as cybercrime, terrorist attacks, human trafficking, online child pornography and drug manufacturing in clandestine laboratories (Ezeji, 2016: 216).

Crime analysts use crime scripts that can be constructed from incomplete data without any specialised software. Ezeji (2016: 216) indicates that a crime script helps to identify additional information that can be helpful to understand crime flow and can be updated if that information is required. It is used to identify opportunities to impede crime incidents by identifying commonalities that are trans-borders to different crime incidents (Ratcliffe, 2016: 102). The police use situational crime prevention measures to prevent cybercrime and to identify possible responses based on situational crime prevention techniques. According to Meyer (2013: 9) the police identify mobile phone service providers that can be used to block calls from certain numbers or prevent them from sharing information about cybercrime activities. Crime scripts can be divided into categories that take place simultaneously or at the same location rather than to conceptualise a crime as a single moment, as it is a process that results from a sequence of previous decisions and have some aftermath. Ratcliffe (2016: 102) states that the use of crime scripts in policing is to deconstruct crime into components and actions that can be individually assessed for their susceptibility as police tactics or crime prevention intervention.

3.10.4 The use of Hypothesis by Crime Analysts to Understand Cybercrime

A hypothesis is a statement of assumed or predicted existence or non-existence of a relationship between variables. Townsley et al. (2012: 140) state that a hypothesis is known as information logic, reason, experimental analysis and communication outcomes that encourage replication. Hypothesis testing is used in policing to streamline the use of analysis technologies because it is relevant in the empirical investigation and it is pragmatic to use scientific principles for cybercrime reduction. It uses the process of strategic thinking and refining the analytical technique as a way of turning everything about a crime into something more specific and actionable (Ezeji, 2017: 216).

An analytical technique helps crime analysts to avoid embarking on large quantities of data, thus spending more time and effort in collecting data and processing them, only to find out at a later stage that much of the collected data are of marginal value to the requirements. Therefore, hypothesis testing helps analysts to be focused on the collected data to produce the results that are useful to arrive at conclusions (Ratcliffe, 2016: 103). Chainey (2012: 110) asserts that effective hypotheses are those that are

directly linked to the crime problem and focus on issues that decision-makers can address. In the police domain hypothesis testing is a new approach that is used to streamline analysis techniques and make them more relevant, therefore the use of analytical techniques is likely to grow as crime scene principles and these techniques will become more embedded in the policing domain (Ratcliffe, 2016: 103).

3.11 TECHNOLOGY ASSOCIATED WITH INTELLIGENCE-LED POLICING TO COMBAT CYBERCRIME

Ezeji (2017: 202) states that the use of technology in policing helps the police to access critical intelligence electronically in real time, complete cybercrime reports electronically in order to receive and respond to individuals and groups about crime incidents. The use of technology has emerged in every aspect of life and the police also include technology to combat cybercrime. It helps police to improve effectiveness and efficiency to respond to the increasing demands of cybercrime problems, sharing information about cybercrime incidents with external agencies and it assists with accountability and management (Evans, 2012: 141). The use of technology in policing has facilitated telephone analyses, tracking of electronic financial transactions, plotting of people movement with airline systems and video surveillance tied to facial recognition to combat cyber -related incidents (Ezeji, 2017: 199). Stainer (2013: 81) believes that technology focuses on the tactical application rather than on strategic value; the focus being on cybercrime hotspots down to cybercriminals profiling, crime mapping, as well as to the estimation of places of cybercrime victimization.

The use of a geographical information system in policing makes things easier and quicker for police to map as many as possible geocoded crime locations in a few minutes. It helps police to apply interpolation tactics that map not just crime points but also with identifying crime hotspots (Ratcliffe, 2016: 145). According to Evans (2012: 142), technology can help the police to combat cybercrime by creating temperature maps of crime that identify hot and cold areas and it can also help in the growth of hotspot policing; in other words, being used by the police to obtain larger quantities of data that are stored in the crime dockets, reports, and crime locations and extract data through time, date, modus operandi and crime queries on the geographical information system (Matsaung, 2019: 17). The use of a geographical information system in policing can assist in mapping cybercrime incidents to identify cybercrime

hot spots, help in cybercrime prevention responses and understand cybercrime distribution. Technology can help the police in monitoring the impact of crime prevention and enables the public to access crime statistics online (Santos, 2013: 95). A geographical information system associated with police accountability in which most police activities are in the virtual context and e-policing personnel understand crimes that occur online, places the police on the crime location at the right time, and helps to understand crime problems and effectively guide police action with the production of a geographical information system to combat crime (Ezeji, 2017: 203).

Ratcliffe (2016: 151) indicates that technology is used to predict the exact location of crime hot spots and helps the police in understanding the types of crime incidents that occur in different locations. It uses historical data to create a spatiotemporal forecast of crime locations to direct police resource allocation decisions with the expectations that the police will be on the crime locations at the right time to detect crime activities and to predict offenders' locations (Ratcliffe, 2014: 4). Technology facilitates a crime prevention strategy to reduce crime through predicting it, using predictive software - algorithms - to predict crime better and guide the police command system to identify and deploy strategies to reduce it (Ezeji, 2017: 204). Prediction can be used to determine the long-term and repetitive crime incidents to identify where crime occurred previously (Ratcliffe, 2016: 152). For the prediction to be effective, it necessitates the police to have more resources such as a predicting software directed to cybercrime incidents and cyber threat intelligence software integrated into an effective decision-making system that knows how to use that product for analysis (Evans, 2012: 142).

Law enforcement agencies around the world embrace the use of the internet and social media to interact with the public online. Most people use electronic devices for mass communication and the police use social media and the internet to share crime statistics with citizens electronically and to trace criminal activities on social media (Ratcliffe, 2016: 152). Social media provides a platform the police can use to engage with communities in real time by means of Online Forums, Chatrooms, Facebook, Twitter and WhatsApp, as well as the traditional ways of posting instant messages on the sites that can be viewed at a later stage (Kelly & Finlayson, 2015: NP). According to Chainey (2012: 81), the police can engage with communities on social media without their knowledge to reach out to groups in innovative ways to map cybercrime

and gather intelligence related to cyber incidents. Social media become an effective police platform that can be used as medium of communication to communicate with the public, monitoring public events for possible cyber- related incidents and targeting cybercriminals on the public Facebook pages. This platform can help police to build cybercrime cases, identify cybercriminal gangs, investigate and gather intelligence related to cyber incidents (Ezeji, 2017: 204-205). Therefore, crime intelligence officers can join public Facebook pages by creating fictitious Facebook personalities to request friendship with cyber gangs; and, once the friendship has been accepted intelligence officers have access to the Facebook entries and may be able to identify cyber gangs' families, criminal networks, photographs and videos. This can assist the police to build social network pictures of criminal gang networks and criminal cases based on the videos and photographs (Ratcliffe, 2016: 153).

3.12 CONCLUSION

Intelligence-Led Policing is the most suitable and innovative tool to deal with cybercrime, transactional crime, organised crime, terrorist attacks and financial crime. It is a valuable policing tool in detecting, preventing and investigating cybercrime and has features of multijurisdictional threats, driven analysis and focus on predicting future crimes. This crime prevention approach has the capability to effect link analysis, commodity flow, transaction analysis and association analysis that focus on the business enterprises of cybercriminals. It can be applied in any policing approach where there are cybercrime problems to understand the true causal factors and an intelligence-led strategy that can help to reduce the adverse effects of cybercrime on the public.

Intelligence-Led Policing has the capability to address the broader cybercrime problem range, to focus more on targeting offenders with a greater emphasis on the enforcement, rendering this policing business model a combination of both crime analysis and criminal intelligence that works with an information management framework as well as analysts to influence decision-making. The ultimate aim of long-term cybercrime prevention solution is to draw from evidence base activities; being a crime prevention model moving to become the vehicle of all-crimes, all-hazards and all-harms business that face many in policing agencies around the world.

CHAPTER FOUR: INTERNATIONAL PERSPECTIVE ON THE POLICING OF CYBERCRIME AND INTELLIGENCE-LED POLICING

4.1 INTRODUCTION

Cybercrime constitutes an international dimension in which criminals send e-mails with illegal content in cyberspace which may pass through different countries during the communication between sender and recipient and this illegal content may be stored outside different countries (International Telecommunication Union, 2012: 3). The use of information technology infrastructure like computers and other electronic devices increases more criminality and puts potential victims at risk of being targeted in cyberspace. Crimes that are committed by means of information technology are high-tech crimes, terrorism, e-crime and cybercrime (Basdeo et al., 2014: 49). The threat of cybercrime is growing at an alarming rate, comparable with the growth of information technology. Countries experience various cybercrime incidents that contribute to more criminality in the countries involved and this kind of crime does not respect any national borders because it is committed in cyberspace (Kigerl, 2012: 470). The prevention of cybercrime requires collaboration between law enforcement agencies and private institutions across national and international borders to drive cybercrime prevention strategies (Dlamini & Mbambo, 2019b: 147). Combating crime is the responsibility of law enforcement agencies but when it comes to crimes such as counterfeit goods and cybercrime it seems as if they do not receive the priority that they deserve (Thenga, 2018: 40).

The use of Intelligence-Led Policing in combating crime is based on developing an investigative methodology that can be used as operational and strategic business model to help police address crime problems, and to guide police and crime analysts to understand the modus operandi of criminals to tackle crime effectively to have a greater impact. It gives the police the opportunity to place threats and risks of crime in the broader context and to assess the social harm of criminality to develop crime preventative measures (Ezeji, 2017: 193).

This chapter focuses on international perspectives on the policing of cybercrime and Intelligence-Led Policing in different countries. The focus will be on countries like the United Kingdom, United States of America, Australia and South Africa. It will also

highlight international frameworks and conventions on the policing of cybercrime through Intelligence-Led Policing.

4.2 BEST PRACTICES FROM SELECTED COUNTRIES ON THE POLICING OF CYBERCRIME

Many countries in the world are globalising their relations and businesses are internationalising their operations to grow in the global market and to compete with others to grow their revenue in the global market. In the same vein, criminals use various tactics to commit various crimes as a way of maximising their ill-gotten profits, as crime remains an attractive business to enrich the free riders financially (Thenga, 2018: 40). Cybercrime is one of the most dangerous crimes in the world and feared by individuals, companies, organisations and governments alike, as it poses security threats for information technology worldwide and it is difficult for law enforcement agencies to detect and combat it because of its border-less nature. This crime requires expertise and cyber-security skills amongst law enforcement agencies around the globe to tackle it successfully (Akdermir, Sungur & Basaranel, 2020:113). As a result of the serious nature of cybercrime, its global nature and implications, it necessitates law enforcement agencies to have a common understanding of its activities globally to be able to deal with it effectively (Alkaabi, 2010: iii).

4.2.1 The policing of cybercrime in United Kingdom

The police in the United Kingdom use the Computer Misuse Act of 1990 to combat computer-related crimes. According to this Act, it is a crime for a person to access a computer or any electronic device or data kept on the computer or electronic device without authorisation for the purpose of committing computer-related crimes or for unauthorised use of a computer to modify contents, data or programmes (Alkaabi, 2010: 31). This Act also criminalises the supply of hardware, software and data that can be used to commit any computer-related crimes. The penalty for the unauthorised access to computer systems is two years imprisonment, while that of the denial-of-service attacks is ten years' imprisonment (Cassim, 2009: 47).

In 2013 the United Kingdom formed the National Cyber Crime Unit under the command and control of the National Crime Agency. The Computer Misuse Act of 1990 empowers the National Cyber Crime Unit as well as other law enforcement

agencies across the United Kingdom and international law enforcement agencies such as the International Criminal Police Organisation, the US Secret Service, the European Union Agency for Law Enforcement Cooperation and the Federal Bureau of Investigation to combat cybercrime activities effectively (White & Goodman, 2021: 33-34). It empowers cybercrime investigators to identify and trace individuals and groups of criminals involved in cybercrime and to raise awareness campaigns in individuals or youth about the consequences of being involved in cybercrime activities. To empower citizens on how to protect themselves from cyber criminality as well as law enforcement agencies to understand the current and emerging threats of cybercrime (White & Goodmen, 2021: 34).

The National Crime Agency in the United Kingdom is a non-ministerial governmental department that reports directly to the Home Office Secretary whose responsibility is to direct the strategies of the National Crime Agency (Brants, Jackson & Wilson, 2020: 457). The main responsibility of the National Crime Agency in the United Kingdom is to direct police operations (guided by Home Office Secretary) to work with police force across the United Kingdom and other law enforcement agencies in coordinating the response to crime, including cybercrime threats (Brants et al., 2020: 457). The United Kingdom's Strategy for Counter-Terrorism (2011: NP) indicates that law enforcement agencies in the United Kingdom use the National Security Strategy to pursue, prevent, protect and combat cybercrime activities. Through this strategy (National Security Strategy) they are able to pursue investigations of cybercrime and disrupt cybercrime activities, conduct public awareness campaigns about the dangers of cybercrime and prepare them to respond to the current and emerging cybercrime, as well as providing support to victims of cybercrime (White & Goodman, 2021: 34).

4.2.2 The policing of cybercrime in the United States of America

Alkaabi (2010: 32) states that the United States of America introduced the Computer Fraud and Abuse Act of 1986 to deal with computer -related crimes and the digital transmission of electronic data to broaden government power to have access to private communication. It was followed by the National Information Infrastructure Protection Act of 1996 to address cybercrime that criminalises acts such as cyber fraud, identity theft, spamming, cyber stalking, making intentional false representations online, the use of password sniffers, the decimation and creation of

worms together with the writing of viruses, Trojan horses, website defacements and web-spoofing (Cassim, 2009: 43). The law enforcement agencies in the United States of America such as the US Secret Service and the Federal Bureau of Investigation use jurisdiction offences under the National Information Protection Act of 1996 and the US Patriot Act of 2001 to address cybercrime within the country (Cassim, 2009: 43). The United States of America joined the European Council as a member of cybercrime on 29 September 2006 and on 1 January 2007 President George Walker Bush signed the Convention to come into force (US Department of Justice, 2008:NP).

The United States of America established the Internet Crime Computer Centre to receive, develop and refer any cybercrime related complaints to the federal government and local police stations across the country. This centre forged partnerships with the Federal Bureau of Investigation and the National White Collar Crime Centre in the reporting of complaints on computer- related crimes (US Department of Justice, 2008: NP). The United States has law enforcement agencies that are responsible for combating cyber- related crimes and deal with digital evidence, namely:

- The Federal Bureau of Investigation - investigates cybercrime incidents, supplies advice, guidance, policies and resources to other law enforcement agencies on the investigation of cybercrime (Alkaabi, 2010: 47).
- Computer Crime and Intellectual Property Section - searches, seizes computers and obtains electronic evidence in criminal investigation (Ritter, 2006: NP).
- National Institutes of Justice - guides law enforcement agencies on how to deal with the collected digital evidence (National Institutes of Justice, 2001: 13).
- The Secret Service - investigates incidents related to cybercrime such as counterfeiting of currency and internet fraud (US Department of Justice, 2008: NP).

- National Institutes of Standards and Technology - ensures that there are standard procedures and measures in place for computer forensic tools to provide evaluation and verification of the tools used to investigate computer crimes and provide valid results (National Institutes of Standards and Technology, 2003:NP).

4.2.3 The policing of cybercrime in Australia

The first Act introduced to deal with computer crime in Australia is the Criminal Code Act of 1989 of Queensland, that deals with computer- related crimes such as cyber stalking, stealing information, internet fraud, unlawful obtaining of information, computer hacking and misuse (Alkaabi, 2010: 30). In 1991 Australia introduced the Telecommunication Act of 1991 that introduced section 74 and 76 into the Criminal Code Act of 1989. Section 74 of the Criminal Code criminalises the producing, supplying and obtaining of data with the intention to commit crime. It also criminalises computer fraud, stalking and computer hacking, while section 76 of the Criminal Code of 1989 criminalises the access to computer systems without authorisation to examine, modify and damage data (Kim, 1997: NP). In 1995 Australia amended the Criminal Code Act by criminalising other computer crimes such as hacking and spreading of viruses (Chan, Coronel & Ong, 2003: 26). When the Australia government realised the ineffectiveness of the current laws to deal with computer crimes, they introduced other laws such as the Criminal Code Act of 1995 and the Cybercrime Act of 2001 to keep up with modern technological challenges (Chan et al., 2003: 25). The Criminal Code Act criminalises the access to other people's computers in order to alter, modify contents to commit computer crime, impair electronic communication without permission, access computers to restrict data or to obtain data from a computer to commit cybercrime (Alkaabi, 2010: 29-30). The Cybercrime Act criminalises the access to impair data that is either stored on the computer or computer disk, to be in possession and control of data with the intention to commit cybercrime, as well as supplying and obtaining such data to commit any computer- related crimes (Alkaabi, 2010: 29-30). Cassim (2009: 49) states that this Act plays an important role in protecting computer systems against cybercriminals, as well as protecting the integrity of the system that processes and stores information.

The Australian Federal Police launched a High-Tech Crime Centre on 2 July 2003 that is responsible for combating, tracing and investigating cyber-related crimes within or outside the country. The centre provides assistance to the local, provincial and national police departments in combating cybercrime because cybercrime occurs at multi-jurisdictional level (Alkaabi, 2010:34). The Australian Federal Police detect, trace, prevent, investigate and coordinate the fight against cybercrime with international agencies and local agencies within Australia. According to the Australian High-Tech Crime Centre (2007: NP), the Australian police focus on unauthorised system intrusion, interruption and destruction that happens within or outside the country or wherever the offender is.

4.2.4 The policing of cybercrime in South Africa

Policing of cybercrime in South Africa relies on various legislations such as the Electronic Communications and Transactions Act No 25 of 2002 (ECT), the Regulation of Interception Act No 70 of 2002 (RICA), the Protection of Personal Information Act No 4 of 2013 (POPIA), the Prevention of Organised Crime Act No 38 of 1999 (POCA) and the Cybercrime and Security Bill to address cyber-related crimes within the country (Van Niekerk, 2017: 115). Section 86 (1) to 86 (4) of ECT Act No 25 of 2002 criminalises the intentional causing of the denial-of-service attacks on legitimate users. In addition, it criminalises unauthorised access or the modification or utilization of programmes to overcome security measures against computer system. The sanction of this offence under ECT Act No 25 of 2002, section 86 (1) provides for a maximum period of one year imprisonment or fine and under section 86 (4) prescribes a fine or imprisonment not exceeding five years. Ezeji (2014: 80) indicates that this penalty has been criticised by various political parties as a lenient punishment that does not deter the public from committing cybercrime. The Regulation of Interception Act 70 of 2002 obliges cell phone users to register SIM cards with respective networks as from 1 August 2009. The purpose of this Act is to help the police to identify and trace any person who uses a cell phone to plan the commission of crime or to trace transactions made during the commission of crime. In terms of section 39 of the RICA Act, any person who failed to comply with the registration of the SIM cards as required were to be disconnected from the network. The penalties under section 51 of RICA are fines not more than two million rand or imprisonment of not more than 10 years. In terms of a juristic person, fines may increase to the amount of five million rand. However, this

sanction of RICA is inadequate in its own to effectively deal with cybercrime (Cassim, 2012: 399).

The purpose of the POPI Act 4 of 2013 is to protect personal information, which is used by either private or public entities. According to Cassim (2015: 78), the POPI Act protects the rights of any person against unlawful electronic communication, it provides conditions to which minimum requirements apply for the processing of personal information and regulates the flow of personal information across the borders of South Africa. Thus, the Act safeguards personal information integrity to protect the damage, alteration and access to information without authorisation by legitimate users (Jideani, 2018: 37). The Act protects personal information and helps the public in general to balance the right of privacy with other rights in accessing the required information. However, the Act has some provisions for the transfer of personal information outside South Africa and data protection compliance provisions enforcement, such as the concomitant offences, penalties and administration fines to those offenders who contravene the Act (Minnaar, 2020: 43). Any person who contravenes the POPI Act can be fined up to R10 million or imprisonment up to 10 years (Cassim, 2015: 80). The Act protects people against any breach of personal and private information. It established an information regulator to monitor and enforce compliance in the violation of personal information (Chitimira & Ncube, 2021: 15). The information regulator ensures that the minimum requirements of obtaining personal information are complied with by people processing personal information. Its duties include providing rules, codes of conduct, procedures on how personal information is processed, providing guidance to people in relation to unsolicited electronic communication, act on the violation of personal information and oversee the flow of information within South Africa (Abiodun, 2020: 41). However, the POPI Act is used in South Africa to protect personal information, and it can help in addressing identity theft and to prevent people to use personal information without authorisation (Cassim, 2015: 80).

According to Minnaar (2020: 43), the use of the POPI Act and the ECT Act to enforce the law on information security and protection are steps in the right direction in combating cybercrime in South Africa (Minnaar, 2020: 43). The Cybercrime and Cyber-security Bill of 2015 criminalises the unlawful and intentional access of

electronic data, computer devices, a computer network and database without permission. The Bill also criminalises the unlawful possession of illegal software with the aim to break a computer device, compromise a computer database and computer firewalls for the purpose of access of personal information. Therefore, this Bill gives the power to law enforcement agencies to search, seize and investigate any information related to cybercrime (Dlamini & Mbambo, 2019b: 149). In terms of the Cybercrime and Cyber-Security Bill of 2015, any person found guilty of cybercrime can be given fine of R5 million to R10 million or imprisonment of 5 years to 10 years or both the fine and imprisonment (Schultz, 2016: 35).

Jideani (2018: 38) states that the Bill also provides the power to law enforcement agencies to investigate cyber- related crime, establish cybercrime structures such as a Cyber-security Hub and Computer Emergency Response Team to ensure it promotes cyber-security capacity building. It protects critical infrastructure against cybercrime, provides a 24/7 cybercrime response mechanism centre and also ensures that electronic service providers and financial institutions comply with the Cybercrime and Cyber-security Bill regulation to assist in cybercrime prevention. According to Schultz (2016, 32), the Bill empowers the police to investigate, search, access or seize anything and it regulates relationships between countries in terms of international cooperation to investigate cybercrime, providing jurisdiction and various structures to deal with cyber-security and regulate National Critical Information in relation to imposing obligation on electronic communication service providers regarding issues that impact on cyber-security.

The Cybercrime and Cyber-Security Bill 6 of 2017 criminalises offences committed by means of computer systems or electronic devices such as hacking, unlawful interception of data, ransom ware, cyber forgery and uttering cyber extortion (Ntsaluba, 2017: 74). The Bill provides rules and regulations that have to be taken into consideration when dealing with cybercrime such as the distribution of data messages which are harmful, providing interim protection orders, regulating structures that deal with cyber- related crimes, the power to investigate such crimes and enforce law to report cybercrime. Bogopa (2020, 7-8) states that the Bill provides mutual agreements between countries to promote measures that can be used for the detection, prevention, mitigation and investigation of cybercrime. The Bill gives the

police power to investigate, search, access and seize anything that can be evidence of cyber- related crimes in any place where it can be located, whether they have a search warrant or not. Ntsaluba (2017: 74) states that the Bill requires the cooperation of foreign states in the investigation of cybercrime and empowers the Minister of Police to detect, prevent and investigate cybercrime 24/7, thereby giving the Minister the power to take appropriate measures to build capacity to ensure that incidents of cybercrime are effectively dealt with and creating mechanisms for cooperation and mutual assistance with law enforcement agencies of foreign countries for the prevention and investigation of cybercrime in South Africa (Chitimira & Ncube, 2021: 19).

The Cybercrime Act 19 of 2020 makes it an offence for any person to access a device or computer system unlawfully, to intercept data unlawfully, to possess a software or hardware tool to commit an offence, to use electronic devices unlawfully to interfere with data, or to use computer systems unlawfully for the acquisition of data. Lambrechts (2021b: 22) states that the unlawful possession or receipt of a password or accessing the code of another person's computer to commit cyber fraud, cyber forgery, uttering, cyber extortion, aggravated offences and theft of incorporeal property are acts of cybercrime. This Act establishes offences that are applicable to cybercrime, but also criminalises the distribution of harmful messages in the public domain without authorisation and it regulates law enforcement and investigative jurisdictions in terms of cybercrime activities (Minnaar, 2020: 43). The Act also obliges organisations, institutions, companies and individuals who become aware that their computers are used for cybercrime activities to report such to the police, and where possible such report should be made not later than 72 hours after discovering it (Minnaar, 2020: 48).

Section 11(1) of the Cybercrime Act 19 of 2020 states that any person found guilty of cybercrime can be fined or sentenced to a period not exceeding 15 years imprisonment or both a fine and imprisonment. The Act empowers the police to enter any place to search and seize any device believed to be evidence of cybercrime for the purpose of prevention or investigation of crime with or without warrant (Lambrechts, 2021a: 38-39). Chitimira and Ncube (2021: 20) indicate that it is the responsibility of the police to participate in the development of anti-cybercrime strategies in South Africa to have specialised training and investigative capacity and

to interact with foreign countries in combating cyber- related crime. The Minister of Police could establish a contact centre which must operate on a twenty-four hour and seven-day-a-week basis to aid in the investigation of cybercrime incidents and to provide advice in the investigation of cybercrime to identify and locate cybercriminals by cooperating with law enforcement agencies internationally. Chitimira and Ncube (2021: 20-21) further assert that the contact centre could ensure that all incidents of cybercrime are reported to the police for further investigation.

4.3 INTERNATIONAL LEGAL FRAMEWORK ON THE POLICING OF CYBERCRIME

Cybercrime poses serious challenges to law enforcement agencies all over the world due to its ability to be committed anywhere in the world at any time, thus making it difficult for law enforcement agencies to identify and prosecute offenders, as they might be residing in a different country than that of their victims. According to Aphane and Mofokeng (2021: 168), it is difficult to prosecute offenders of cybercrime because different countries have different laws and it is challenging to apprehend offenders without mutual agreements on extradition. Cybercrimes are known to be increasingly becoming major threats to computer systems in the ever -changing era of digital technology. Alkaabi (2010: 28) points out that countries are forced to re-examine their legal systems to determine their effectiveness as cybercrime threats are constantly growing. Dlamini and Mbambo (2019b: 146) explain that Western countries make progress in developing policies that can be used to combat cybercrime, but legislation to deal with cybercrime is limited to the country of implementation as domestic legislation only applies to that particular country and the implementation of cybercrime policies is highly dependent on that country's interpretation. There is a need for countries to harmonise and streamline cybercrime laws and policies to be effective in dealing with cyber criminality. Cassim (2009: 41) opines that the aim of conventions such as the Council of Europe's Convention and United Nations Convention against Transnational Organised crime is to encourage international cooperation amongst the countries to comply with the integrity of the internet and to address the global problem of cybercrime (Cassim, 2009: 41). If countries become members of conventions, it would be one step towards combating transnational organised crime, indicating to other states that member states also have serious challenges with this crime and they would recognise the need to foster relations with other countries for international

cooperation in combating this crime (Thenga, 2018: 51-52). This sentiment is supported by Alkaabi (2010: 23-24) who also states that for countries to combat cybercrime successfully they need to forge relations with international organisations such as the Council of Europe Convention on cybercrime, the United Nation convention, the African Union International Telecommunication Union and the Group of Eight (G8).

4.3.1 The Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime is the first international treaty on crime and it requires international co-operation amongst countries on cyber policies to ensure that the integrity of the internet is protected to address the global nature of cybercrime. The convention deals with crimes through the internet and other computer networks, especially crimes related to infringements of copyright, computer fraud, child pornography and violation of computer security. The focus of this convention is to protect society against cybercrime and to enforce the laws of cybercrime at an international level (Cassim, 2009: 41-42). The convention of cybercrime was introduced by the Council of Europe member countries and four non-European countries such as South Africa, Canada, the United States and Japan. It was signed on 23 November 2001 by Europe and non-Europe member countries, while the United States ratified it in September 2006 and it came into operation in January 2007 (Basdeo et al., 2014: 51). This convention deals with substantive and procedural legislation that focuses on criminal activities domestically and transnationally. It promotes training of law enforcement personnel, improves cooperation between cybercrime stakeholders and law enforcement agencies and engage with community-led initiatives to combat cybercrime (Alkaabi, 2010: 25). South Africa signed the convention to become a member state but never ratified it. The convention encourages member states to incorporate the international laws on cybercrime into domestic laws (Schultz, 2016: 19). Dlamini and Mbambo (2019a: 4) agree that South Africa complied with the first part of the convention by criminalising cybercrime and introducing the Electronic Communications Transactions Act 25 of 2002 in combating cybercrime.

The Budapest Convention provides member states with guidelines on how to develop their own national legislation on cybercrime, to establish anti-cybercrime frameworks, to implement adequate laws on cybercrime applied globally amongst member states,

to empower investigators to improve investigation techniques and to interact with member states to increase international cooperation (Chitimira & Ncube, 2021: 5-6). According to Ntsabula (2017: 42), the convention focuses on substantive law provisions that are against computer crime, child pornography and copyright infringement at an international level. It also provides procedural law that balances the violation of human rights and provides evidence on computer crime to the law enforcement agencies for successful prosecution. Besdeo et al. (2014: 51) argue that the aim of this convention is to combat cybercrime and allow member countries to identify substantive offences and develop domestic procedural laws that can be used to investigate cybercrime, address cybercrime that occurs on international level and assists in the international cooperation, as well as criminal investigation and extradition of cybercriminals. According to Alkaabi (2010: 26), the Council of Europe Convention on Cybercrime requires member states to formulate laws that can be used to combat cybercrime and to ensure that there are capable law enforcement agencies to investigate and prosecute cybercrime in collaboration with other law enforcement agencies (Alkaabi, 2010: 26). The council plays a dominant role at an international level to address cybercrime by strengthening cooperation amongst the member of states, providing coordinated financial needs for training activities amongst law enforcement, forge partnership with private institutions to fight cybercrime and monitor the trends of cybercrime to evaluate the prevention measures (International Telecommunications Union, 2012: 130).

4.3.2 The United Nations Convention

The United Nation Convention against Transactional Organised Crime was established on 15 November 2000 under the general assembly resolution 55/25. It is an international instrument in the fight against transnational organised crime (United Nation, 2004: iii-iv). The convention has three protocols that specifically deal with organised crime, such as the protocol to prevent, suppress and punish trafficking in people, especially women and children; the protocol against the smuggling of migrants either through land, sea and air and the protocol against the illicit manufacturing of and trafficking in firearms, including parts and components of ammunition (United Nation, 2004: 2-7). The convention also outlines steps to be taken to fight transnational organised crime and stresses the need by its members to understand the seriousness imposed by transnational organised crime in an attempt to foster partnerships and

close international cooperation combating this crime (Thenga, 2018: 52). The United Nations is an international organisation that supports countries to establish the collaboration of international law, including security, economic development, social progress and addressing human rights violations. However, the United Nations established organisations such as the United Nations Office on Drugs and Crime (UNODC) to assist member states to combat crime and the UN Convention against Transnational Organised Crime which focuses on combating transnational crime. The mandate of this organisation is to provide the legal framework at an international level for cooperation amongst countries in combating criminal activities and identifying the relation between terrorist crimes and transnational crime (Alkaabi, 2010: 23).

The United Nation produced a report on effective measures that can be used in preventing and controlling high-technology and computer- related crime. This report recommended that strategies should be constituted that can be used to enhance international cooperation to counter and prevent computer crime (Alkaabi, 2010: 23). The United Nation Convention on Cybercrime was established by the General Assembly Resolution 74/247 in 2019 to elaborate on the Comprehensive International Convention in combating the use of Information and Communication Technologies in committing crime. This was to promote international cooperation in the fight against cybercrime that has become increasingly complex in nature (New Zealand Ministry of Justice, 2019: 1). It also has to ensure that member states comply with the laws and practices to eliminate safe havens for cybercriminals and that law enforcement agencies should cooperate in cybercrime investigation and prosecution. Member states are expected to have cybercrime laws in place that protect the confidentiality, integrity and availability of data, and that computer systems should always be protected from unauthorised impairment (Nduka & Basdeo, 2021: 7). Member states are also encouraged to work with other international and regional organisations in developing laws, policies and practices that deal with cybercrime (Nduka & Basdeo, 2021: 7).

4.3.3 African Union

The Organisation of African Unity was formed in Addis Ababa on 25 May 1963 to promote unity and solidarity among African countries. It also promotes international cooperation based on the Charter of the United Nations and the Universal Declaration

of Human Rights, as well as promoting the co-ordination and harmonisation of other things such as political, diplomatic, economic, cultural, education, welfare and defence policies (Thenga, 2018: 55). The Organisation of African Unity was replaced by the African Union in 2002, which among other, aims to promote fundamental principles of sovereign quality, achievement of greater unity and solidarity among Africa states and to promote peace, security and stability in African countries. It also provides conflict resolutions to the African countries against war crimes, genocide and crimes against humanity to ensure that intervention takes place to restore peace and security (Montesh, 2019: 81).

The African Union established a legal framework for cyber security in African countries to address cyber legislation. The purpose of the African Union Convention is to harmonise African cyber legislation such as e-commerce, protection of personal data, cyber-security promotion and cybercrime (Schultz, 2016: 20). The African Union Convention criminalises the use of identity flexibility that is associated with anonymity in the e-commerce, to address the use of encryption in cybercrime and to prohibit any discrimination that occurs online. It further provides for independent experts who are responsible for vulnerability testing of internet services, establishing processes that can be applied in Africa's Information Communication Technology and development to incorporate online security measures proactively (Ntsabula, 2017: 46-47). The Malabo Protocol (formerly known as the Africa Union Convention) is a legal framework for cybercrime on African countries to fight against criminal activities such as cybercrime and money laundering. It assists African countries to devise preventative measures against cybercrime while observing the basic freedom of and the protection of human rights, as well as taking into consideration the security needs of the people (Walker, Allen, Abderrahmane & Yared, 2021: 5). The African Union introduced the draft of the African Union Convention in 2011 to strengthen existing laws on information and communication technology. Its mandate is not limited to combating cybercrime, but also focuses on other information technology issues such as data protection and electronic transactions. The convention deals with electronic commerce which addresses contractual responsibility of an electronic service provider, treaty obligations in electronic form and the security of electronic transactions as well as data protection and issues related to cybercrime (International telecommunication Union, 2012: 138).

4.3.4 The International Telecommunication Union

The International Telecommunication Union (ITU) was formed by the United Nations (UN) to specialise in the development of the Global Information and Technology footprint. According to Alkaabi (2010: 24), it is a specialised agency of the UN that coordinates the global use of telecommunication and improve telecommunication infrastructure for developing countries and it also deals with cyber-security challenges. It was established to deal with the information technology of governments and the private sector to improve the development and standardisation of telecommunication networks and services, as well as protecting the information of society (Ntsabula, 2017: 43). The International Telecommunication Union (2012: 121) states that the ITU is a specialised agency within the United Nations that standardises and develops communication that deals with cyber-security matters. The ITU gave rise to the establishment of the World Summit on the Information Society (WSIS) that took place in Switzerland in 2003 and in Tunisia in 2005. The role of the WSIS is to ensure that policy decision makers and experts come together to share ideas and experiences on how best to develop strategies to address improvements and developments of global information in society. The outcomes of the WSIS were published in the Geneva Declaration of principles, the Geneva Plan of Action, the Tunis Commitment and the Tunis Agenda for the Information Society.

According to the International Telecommunication Union (2012: 44), the UN General Assembly provides legal advice to the ITU on cyber-security related matters and information that can be used to co-ordinate the use of multi-stakeholder participation to provide a legal framework for international cooperation and to promote cyber-security to ensure the enhancement of confidence and security information in society. This can help governments, the private sector and other cybercrime prevention stakeholders to have a mutual partnership to detect, prevent and respond to cybercrime and Information Technology. On the other hand, it can help to provide guidelines as ongoing efforts for implementing cybercrime legislation that can help in effective investigation and prosecution, encouraging mutual assistance efforts and promoting international support for preventing, detecting and designing educational programme such as raising awareness about cybercrime. Alkaabi (2010: 24) states that in 2009 the ITU established the toolkit for cybercrime legislation which is used to

provide countries with a strategy that can assist in the implementation of harmonized cybercrime laws and procedural rules. However, in April 2010, the UN members rejected the use of the ITU global cybercrime treaty because there was no agreement among member states on matters such as the transfer of digital evidence on cybercrime. It was indicated that such treaty would take time to resolve cybercrime activities, and the European Union as well as the United States of America were of the view that there was no need for a new treaty because the Council of European Convention was already in existence (Alkaabi, 2010: 24).

4.3.5 Group of Eight (G8)

The G8 is a group of eight rich countries in the world that is composed of Canada, France, Germany, Russia, Italy, Japan, the United Kingdom and the United States of America. Alkaabi (2010: 26) indicates that these countries also discuss the combatting of crime and their main focus is on transnational organised crime, such as cybercrime and other computer- related crimes. The G8 established a subcommittee on high-tech crimes to combat cybercrime and during a subcommittee meeting that was held in Washington DC in the United States, the G8 Justice and Home Affairs Ministers decided to prescribe principles and a Ten-Point Action Plan to address high-tech crimes. These principles and the Ten-Point Action Plan endorsed that there should be no tolerance for people who abuse information technologies and that member states must ensure that the investigation and prosecution of international high-tech crimes are jointly coordinated by concerned states, regardless of where the crime has been committed. In addition, there should be training for law enforcement agencies to be equipped with the skills to address high-tech crimes (International Information Union, 2012: 114). They (G8) established a contact centre at international level that is operational 24/7 to conduct investigations of high-tech crimes to prevent the establishment of lawless digital havens. The International Information Union (2012: 115) states that by doing so, the G8 attempted to follow the legal instrument of the Council of Europe's Convention on Cybercrime by implementing procedural instruments to fight cybercrime, aiming to improve the effectiveness of cybercrime counter- measures. Alkaabi (2010: 26) asserts that the G8 advises member countries on the combating of cybercrime and provides recommendations on how best to review their legislation to ensure that high-tech crimes are prohibited. However, the G8

encourages all member states to implement their own laws on combating organised crime, high-tech crimes and terrorist attacks.

4.4 THE INTERNATIONAL CRIMINAL POLICE ORGANISATION

The International Criminal Police Organisation (INTERPOL) was formed in Vienna in 1923, to provide and promote mutual agreements between law enforcement agencies around the world with certain limits of national laws and the universal declaration of human rights. It serves as a police cooperative network that fosters collaboration and provides assistance in police work among law enforcement agencies around the world (Deflen & Maybin, 2005: 178). Its ultimate aim is to facilitate crime combating for safety and security around the world by providing collaboration within police forces around the world. Thenga (2018: 53) explains that its mission is to combat crime through international cooperation and innovation on police and security matters.

Interpol has 186 member countries and use an International Communication System called 1-24/7, which is used to collaborate with member countries on criminal activities. This enables and facilitates the exchange information on crime among the law enforcement agencies of member states. Cybercrime incidents can also be reported at all times, thus creating secure communication for collecting, sharing, analysing and requesting information that can be retrieved by member countries from the database (Alkaabi, 2010: 27). Interpol offers support to member countries to facilitate the international collaboration among the law enforcement agencies around the world to combat cybercrime. Moreover, Interpol uses international cooperation amongst member countries to share cybercrime information with member countries and build partnerships with international private organisations in combating cybercrime (Alkaabi, 2010: 27).

4.5 THE USE OF INTELLIGENCE-LED POLICING TO COMBAT CRIME IN DIFFERENT COUNTRIES

Transnational organised crime occurs across national borders which involves criminal syndicates working in different countries to execute their illegal business ventures. The most common transnational organised crimes are human trafficking, illegal trade in drugs, smuggling of weapons, endangered species, selling of body parts, terrorist attacks and cybercrime, which are a major concern for most countries and require

urgent intervention from law enforcement agencies (Ezeji, 2017: 174). The above transnational organised crimes require solutions from local and international law enforcement agencies to address this crime through joint collaboration and cooperation (Jackson, 2012: 39). The use of Intelligence-Led Policing in combating crime has been endorsed across the world (Ezeji, 2017: 167). This section focused on the use of Intelligence-Led Policing to combat crime in various countries such as the United Kingdom, the United States of America, Australia and South Africa.

4.5.1 The use of Intelligence-Led Policing in the United Kingdom to combat crime

The sharp increase of crime in the United Kingdom put pressure on the police to be more effective and cost efficient. This pressure emanated from the internal and external factors that led to the implementation of a proactive police strategy which is Intelligence-Led Policing. Considering that internal pressures contributed to the loss of the ability to control crime on the streets and the subsequent criminal takeover of the streets which caused the public to lose confidence in the police to protect them against crime. External pressure caused by poor police leadership that fails to use effective policing style to combat crime resulted in the inability of the police to cope with rapid changes in the global world and this increased the opportunity for transnational organised crime and removed the use of physical and technological barriers across the policing domain (Mashiloane, 2014: 196). The use of Intelligence-Led Policing in the United Kingdom was developed in the 1990 as a strategic innovation for combating crime, especially habitual crime and complex criminality (Carter, 2016: 440). This model was used during the increase of crimes such as property-related offences, for instance burglary and automobile theft. The model focuses on prolific offenders rather than on reported crime as a way of police utilising their resources more effectively (Mugari et al., 2015: 88).

The use of Intelligence-Led Policing to combat crime in the United Kingdom was developed by David Phillips and Brian Flood in 1993 by means of the Kent Policing Model. The Kent Policing model is used to help law enforcement agencies in the collection and analysis of information about criminals and their associates to target them to prevent criminal activities through disruption (Osborn, 2012: 15). The use of the Kent Policing Model promotes the use of proactive policing to combat high volumes

of property and other organised crimes (Wortley & Mazerolle, 2008: 266). David Phillip reiterated that the increase of crime in the United Kingdom required extensive and influential proactive Intelligence-Led Policing initiatives to combat the high rates of crime across the United Kingdom. However, the Kent Policing Model is seen as an Intelligence-Led Policing problem approach to assist in crime reduction and crime-combating techniques as primary objectives (Osborn, 2012: 14-15). Intelligence-Led Policing in the United Kingdom was used by the National Crime Intelligence Service and the Organised Vehicle Crime Programme to combat crime such as motorcycle theft, stolen cars and cloning or the rebadging of stolen cars as legitimate use for sales. Intelligence-Led Policing can be used for that purpose to prevent the stealing, rebranding and reselling of vehicles to West Africa (Lesion, 2012: 7). Britain's National Criminal Intelligence Service (NCIS) uses the National Intelligence Model to address the problem of crime by targeting offenders to ensure that crime scene and disorder hot-spots are properly managed, to investigate any linkage of series of crime and to apply preventive measures correctly which are principles of Intelligence-Led Policing (Mashiloane, 2014: 199).

The United Kingdom uses surveillance and informants as ways to combat crime through disruption activities. Intelligence-Led Policing to combat crime encourages the increased use of surveillance and informants which are prudent to explore the cost benefit techniques (Ratcliff & Guiditti, 2008: 9). Police surveillance deals with organised crime investigation, placing personnel on surveillance, devoting time to those criminals who have not yet committed crime. Ratcliff and Guiditti (2008: 9) indicate that surveillance operations are time-consuming and expensive. The police, however, regard the use of informants to collect information as a viable source of information to combat crime. The police use informants who provide information so that they can get paid and offenders who cooperate hope to get leniency for the crimes that they had committed (Lesion, 2012: 7). According to the Majesty's Inspectorate of Constabulary (2014: 8), informants should be used with necessary discretion and proper supervision to plan crime operations and to understand the criminal environment better through strategic planning.

4.5.2 The use of Intelligence-Led Policing in the United States of America

Intelligence-Led Policing is the latest policing philosophy model that was intensively implemented in the United States of America after the terrorist attack of 11 September 2001. Carter and Fox (2018: 2) attribute the implementation of this model to the failure of law enforcement agencies to share information that led to the 9/11 attack, thus compelling the police to work smarter when dealing with criminals within their available resources. In March 2002 the Investigative Operation Committee of the International Association of Chiefs of Police launched the Intelligence Sharing Summit to introduce the Global Intelligence Group that can be used to develop a criminal intelligence sharing plan (Mugari et al., 2015: 88). The plan had to devise strategies that could be used to promote Intelligence-Led Policing as a blueprint for law enforcement administrators as well as to build an intelligence system and a model for intelligence process policies. However, the plan is used by most law enforcement agencies all over the world to gather and evaluate information and disseminate intelligence products in such a way that protects the individual's rights to privacy while combating organised crime and public disorder (Mugari et al., 2015: 88).

Mashiloane (2014: 206) argues that the tragic terrorist attack in the United States of America was a wake-up call for law enforcement agencies to use a more proactive and cooperative Intelligence-Led Policing model to share crime information to identify crime threats and devise better solutions to prevent those threats. Law enforcement agencies in the United States established Fusion Centres to address domestic problems by means of increasing information and sharing intelligence with local, state, federal and private partners. The Fusion Centre assesses crime and other security issues to determine the trends of crime and to ensure that it conceptualises multi-agency analytic centres of excellence, with the aim of dealing with information and intelligence sharing. Hence, the core function of the Fusion Centres is to receive, gather, analyse and disseminate information to partners to combat terrorism, ensure public safety and homeland security (Ezeji, 2014: 157). The use of Intelligence-Led Policing perspectives by Fusion Centres assists law enforcement, homeland security, the public and private sector and communities to understand the crime environment and to use intelligence products to influence decision makers through analysis and sharing intelligence among state, local and federal governments (Ezeji, 2014: 157).

4.5.3 The use of Intelligence-Led Policing in Australia

The use of Intelligence-Led Policing in Australia to combat crime was adopted as a result of the increase in burglaries in the country and it was put into operation via Operation Anchorage (Heldon, 2002: 6). The main focus of Anchorage Operation is on senior leadership of the police to use their tactics to target recidivists by using crime and intelligence analysis to combat such burglaries (Makkai, Ratcliffe & Lisa, 2004: 6). The Anchorage Operation consists of a number of police officers which include four teams of 10-12 investigators and six intelligence officers to analyse crime patterns and other crime information through the use of covert surveillance and field interviews. The police use intelligence analyses to combat burglaries by targeting suspects every two weeks to ensure that a list of targeted suspects is circulated among them for the purpose of identifying and arresting those suspects. The use of targets assists the police in reducing crime in a shorter period and produces positive results because it involves a significant number of police officers (Ratcliffe, 2007: 6).

The use of Operation Anchorage to combat burglaries in Australia reduced crime in large numbers, as the recorded crime declined for 45 weeks and there were no reported burglaries for that period. This clearly indicated that the use of this operation prevented around 524 burglaries and it further prevented 2, 445 offences of burglaries within a period of 45 weeks after this operation, before crime of burglaries returned to the level it was before Operation Anchorage (Ratcliffe & Makkai, 2004: 19). The use of intelligence analysis in Operation Anchorage yielded positive results in crime reduction and it can do more if it could target prolific and persistent offenders as well.

The use of Intelligence-Led Policing to target recidivists of property crime sustains positive outcomes to combat this crime and to protect the community, thus helping to combat reported crime and thousand other crimes that occur within Australia (Makkai et al., 2004: 22). This operation helps the police to combat crime through situational crime prevention and a problem- oriented approach which help to control crime in both the short-term and long-term (Heldon, 2002: 6). Intelligence-Led Policing is a vehicle that drives proactive policing to address problem- solving activities thus becoming an effective tool to deal with problem solving. It is a model that is guided by crime analysis to identify and trace criminals, as well as identifying hotspots and understanding crime and disorder activities. These activities include operational and non-operational

strategies that can be used to analyse problems, implement and review strategies. According to Mashiloane (2014: 216), these activities require on-going processes to be repeated more than once until the positive results are produced.

4.5.4 The use of Intelligence-Led Policing in South Africa

The rapid globalisation, the spread of communication among criminals and the use of technologies in committing crime contribute to the increase of crime in South Africa (Civilian Secretariat for Police, 2013: 30). High crime levels in the country, especially violent crime, force police to propose solutions that can be used to address crime problems, which is Intelligence-Led Policing to enable them to change crime circumstances and utilise international best practices (Zinn, 2011: 12). The South African Police Service must be a step ahead to beat criminals at their own game by employing both tactical and strategic operations to address crime and criminality. The police need to use Intelligence-Led Policing to reduce and combat crime through the proactive analysis of crime and by using intelligence initiatives for collection, organising and analysis to guide both operational and tactical law enforcement decisions (Budhram, 2016: 91). The increase of organised crime syndicates in South Africa led to the adoption of Intelligence-Led Policing to combat crime in 1995. Crime analysts are employed to identify crime problems by using the crime pattern analysis matrix that in turn feeds into automated crime reporting in the Crime Administration System. Govender (2012: 83) believes that Intelligence-Led Policing can be used to collect information on organised crime activities to link perpetrators by means of the Association Network Analysis Chart that would enable the police to identify perpetrators, including their associates, specific activities and institutions. The police use operational, tactical and strategic intelligence to collect, collate, analyse, coordinate and disseminate information to neutralise, prevent and combat organised crime activities (Budhram, 2016: 89).

Intelligence-Led Policing helps the police in long-term crime prevention planning and to devise strategies to combat crime by applying various crime prevention measures such as visible policing, sector policing and community policing to address crime problems (Zinn, 2010: 121). Mashiloane (2014: 229) supports this by stating that Intelligence-Led Policing is used by the South African Police Service as the core of all policing activities, as it introduces a scientific approach towards combating crime and

ensures that policing resources are used in the most efficient and cost effective manner to support police operations. The South African Police Service use Intelligence-Led Policing to reduce crime through crime analysis and intelligence that enable them to analyse crime information to develop appropriate strategies to detect, prevent and combat crime challenges (Mashiloane, 2014: 137).

Intelligence-Led Policing could also be used in South Africa to combat technology-based crimes such as cybercrime through specialized software packages that could be used to analyze such crimes so that crime analysts can understand them better (Ezeji, & Olutola, 2018: 178). Budhram (2016: 92) opines that the increased use of Intelligence-Led Policing on technology-based crimes in South Africa has been observed in the Banking Sector. The South African Banking Risk Information Centre (SABRIC) was formed by all South African banking industries to combat crimes related to banks. Budhram (2016: 91) further indicates that SABRIC operates as a nodal point between the banking industry on financial crimes related to banks and support banks to address such crimes. It uses the concept of Intelligence-Led Policing to combat corruption related to banks through the collection of crime information by means of sophisticated information technology to identify and profile people who perpetrate crime through the banking industry. Worth noting is the fact that SABRIC provides logistical support only, it cannot arrest, search or seize because that is the duty of the South African Police Service in terms of the South African Constitution, Criminal Procedure Act and the South African Police Act (Budhram, 2016: 92). Budhram (2016:92-93) further explains that the Financial Intelligence Centre that is established in terms of the Financial Intelligence Centre Act 38 of 2001 uses Intelligence-Led Policing to combat finance-related crimes such as money laundering to break the cycle of organised criminal groups that benefit from illegitimate profit.

4.6 CONCLUSION

Countries must learn the best practice to teach each other to deal with cybercrime and use international cybercrime frameworks for success in combating cybercrime. The best practice helps law enforcement agencies around the world to explore the effectiveness of the contributions made by national and international policies in combating cybercrime. To combat cybercrime successfully, law enforcement agencies around the world should use Intelligence-Led Policing to investigate criminal behaviour

so that links and patterns of cybercrime can be established amongst individual crimes to identify cybercrime series.

Intelligence-Led Policing helps law enforcement agencies to take a long-term review for planning cybercrime prevention by applying various techniques such as implementing neighbourhood watch schemes for monitoring cyberspace, using closed circuit television systems to identify cyber-threats and alerting law enforcement agencies to trace illegal contents moving in cyberspace. Intelligence-Led Policing is known as the best crime prevention model to combat crime and the success of it depends on how the host country is implementing it.

CHAPTER FIVE: THE USE OF CRIME ANALYSIS TO COMBAT CYBERCRIME

5.1 INTRODUCTION

In the South African context, crime has become a challenge that is increasingly diverse, sophisticated and difficult to combat. Criminals have become smarter at their game, and criminologists believe that the police require certain knowledge, skills and attitudes that can help them to address crime, criminals and victims (Govender, 2012: 79). As a result of the higher crime levels in the country, communities and businesses believe that the police do not have the required knowledge to protect them against crime (Govender, 2012: 79). The only way the police can combat crime successfully is through proper crime analysis. Mashiloane (2014: 103) states that analysing crime helps to predict future criminal activities, identify and apprehend perpetrators and develop crime prevention strategies that can be helpful to combat crime. Matsaung (2019: 30) also supports this by stating that crime analysis helps the police to understand criminal activities and implement crime prevention strategies that are useful in managing crime, investigating crime and disorder. Such analysis depends on crime information reports provided by the police and other related crime information that is in the public domain to identify and interpret crime patterns and crime trends. Crime patterns could identify offenders, crime types, victims, and the locations where crimes are committed (Newburn, 2003: 340).

The purpose of crime analysis is to provide crime information to the police to deal effectively with crime threats or potential threats, to provide warning of threats on time and support operational activities of policing (Krause, 2007: 17). It is a product of Intelligence-Led Policing that helps the police to prevent, combat and solve crime, and has been used by law enforcement agencies for many years to combat crime. It enables the police to understand criminal activities, to know better about the time and place where crime occurs as well as the rationale for committing such crime. This approach can be used by police as integral part in the prevention and suppression of criminal activities. The use of crime analysis in policing provides the police with an opportunity to obtain more information about criminal activities. Berning and Masiloane (2012: 85) emphasise that crime analysis helps the police to understand the nature and extent of the crime and to devise crime prevention approaches that can be used to prevent, combat and resolve committed crime.

5.2 THE PURPOSE OF CRIME ANALYSIS

Crime analysis is used for the systematic examination of crime, criminal behaviour and disorder problems. Crime analysts use analytical techniques such as qualitative and quantitative methods for data collection and analysis. A qualitative data method is used to examine non-numerical data to find causes of crime, characteristics of crime scenes, to identify individuals who have knowledge about specific crimes and apply content analysis to examine police dockets (Hill & Paynich, 2014: 10). A quantitative method is used to examine numerical data through statistical analysis to understand socio- demographic information, identify the crime scene and to identify both victims and suspects (Santos, 2013: 3). Crime analysts use the quantitative method through statistical analyses like frequencies, percentages, means and rates (Mashiloane, 2014: 109). Crime analysis is an autopsy of the crime activities, and its role is to understand the security threats so that a solution can be provided. It helps to understand and recognise the cause of crime and devise crime reduction and crime prevention strategies (Mashiloane, 2014: 109).

Spatial analysis is used to discover the nature of the crime problem and disorder location that links the relationship between other variables and geographical features of specific locations. On the other hand, crime analysts use temporal analysis to know the nature of crime in details through examining long-term trends of crime on yearly, quarterly, and monthly basis (Santos, 2013: 3). This assists the police in crime prevention and detection efforts, as well as to target criminals. The use of crime analysis in policing is essential to supply the police with information about a crime that has occurred recently, it helps to target offenders by using problem-oriented policing and Intelligence-Led Policing. According to Newburn (2003: 341), the use of Intelligence-Led Policing constitutes a smarter policing approach to deal with organised crime and large volumes of criminal activities to target offenders. Crime analysts use technology and specialised software packages to understand the detailed picture of cybercrime activities by interpreting the trends, patterns and incidents of cybercrime.

5.3 TYPES OF CRIME ANALYSIS IN POLICING

Crime analysis involves the use of uniform techniques that help the police in developing hypotheses, understanding criminal events, determining a series of crime, establishing criminal networks and analysing crime to understand its scope and patterns (Krause, 2007: 24). Horne (2009: 69) asserts that it is a process in which crime analysts study crime patterns and trends to predict how crime affects a particular community and how the police interpret crime for response. It consists of different types, namely - operational crime analysis, administrative crime analysis, tactical crime analysis, strategic crime analysis, investigative crime analysis and intelligence crime analysis. Each type of crime analysis has its own meaning and characteristics of analysing crime, depending on the type of data used, the analysis method and purpose. However, crime analysis has different types and purposes to address crime and disorder problems (Mashiloane, 2014: 113).

5.3.1 Operational crime analysis

Osborne and Wernicke (2003: 10) indicate that operational crime analysis guides the police on how to use the resources more efficiently in areas such as redistricting assignments and budget issues. It focuses on the deployment of staffing and resources to understand the internal operation of the police to minimize inefficiency and to improve effectiveness (Hill & Paynich, 2014: 10). The police use operational analysis as a supporting tool to gather and collect crime information as well as to identify crime trends, patterns, series and sprees that provide them with the investigative leads (Krause, 2007: 10). Operational crime analysis leads to administrative police work such as the deployment of resources like personnel, money and equipment to support the police geographically and organizationally to ensure that deployment of resources influence the combating of crime and disorder problems in their jurisdiction (Santos, 2013: 62). Operational crime analysis can help the police to combat cybercrime activities by determining how crime occurs, time of crime, date of occurrence, which geographical area, suspect personal details and the modus operandi used. This helps the police to arrest suspects, confiscate anything gained from cybercrime activities, target criminal groups, interrupt and prevent future cybercrime.

5.3.2 Administration crime analysis

The use of administrative crime analysis provides the police with accurate crime information that can be used in comparing and bench-marking criminal activities. Collected information is useful to inform decisions on allocating resources, staffing and budgeting to combat crime and deal with criminal activities (Berning & Masiloane, 2012: 86). Some of the focus of administrative crime analysis is to present outcomes of research findings based on the legal, political and practical concerns, as well as to convey information amongst law enforcement administration, municipalities and society (Mashiloane, 2014: 116). According to Matsaung (2019: 33), crime statistics disseminated on the police website are easily accessible to the public and provide a summary of criminal activities. The researcher is of the view that administrative crime analysis is helpful in policing because it could provide information about cybercrime levels to citizens by publishing cybercrime statistics on the police website. Such analysis can assist in summarising the statistics on cybercrime to compare its increase or decrease at different periods of the year or from year to year.

5.3.3 Tactical crime analysis

The police use tactical crime analysis to examine recent criminal activities, analysing where, when and how crime happens and developing strategies that can be used for pattern analysis, crime investigation, identification of suspects and case clearance rate (Santos, 2013: 61). Analysis methods can be employed to develop a predictive approach in identifying potential criminals and put them under surveillance as a form of crime prevention strategy by targeting criminals who intend to commit crime (Hill & Paynich, 2014: 9). According to Osborne and Wernicke (2003: 5), tactical crime analysis is used to respond to crime challenges and to predict future crimes by studying current patterns on criminal activities. It deals with the profiling of offenders, crime pattern detection and linkage analysis with the purpose of preventing crime. Analysis is used on the crime information collected to identify crime trends in the early stage of crime so that profiling of victims and offenders can take place to deal with it (Berning & Masiloane, 2012). Mashiloane (2014: 114) states that tactical crime analysis links similar crimes to determine whether they have similar characteristics with regard to patterns and trends, thus identifying alleged suspects and helping to resolve crime. The researcher is of the view that tactical crime analysis can help the police to examine cybercrime data daily to understand the patterns and trends and

develop investigation leads on recent cybercrime activities. Cybercrime information can be shared among detectives for investigation purposes and arrest of suspects by crime prevention officials for crime prevention purposes.

5.3.4 Strategic crime analysis

Strategic crime analysis deals with long-term crime problems and focuses mainly on the projection of long-term increase or decrease of crime. It uses statistical analysis forecasts on crime to make informed future decisions to increase or decrease the capacity of the police in their daily operations (Krause, 2007: 29). Berning and Masiloane (2012: 86) believe that it employs the crime data that has been collected in the past to provide long-term crime prevention strategies and to do planning. It analyses crime and other law enforcement issues, enables the police to identify long-term crime patterns and disorder problems to assist them to develop a targeted response to crime problems. The collected and analysed information helps the police to understand the root cause of crime and to devise preventative measures to reduce it (Hill & Paynich, 2014: 10). Police management collects crime information over a long period to be used by operational police officers to make informed future decisions and devise future operations to deal with crime and criminality. Krause (2007: 30) states that crime information supports the implementation of priorities regarding emerging crime threats. The researcher believes that strategic crime analysis can help the police to predict medium and long-term threats of cybercrime which will enable them to develop effective measures to deal with those threats, because of its ability to analyse previous and present occurrences to predict the future. It therefore requires the police to collect cybercrime information from multiple sources such as police records, information available in the public domain, demographic data, economic data and the data collected by undercover agents.

5.3.5 Investigative crime analysis

Investigative crime analysis involves discovery of criminal activities, geographical areas and psychological intention that contributed to the crime to identify criminals (Govender, 2011: 123). This analysis is usually used to study serial criminals or unknown offenders to discover crime scene locations as well as the physical areas of both offenders and victims and to develop crime patterns to link crimes and address serial criminal activities.

Investigative crime analysis aims to profile serial criminals at national, provincial and police station precincts to determine crime patterns to understand the nature of crime, facts of the case and to determine characteristics of victims and criminals alike (Mashiloane, 2014: 117). This analysis assists in the investigation of cases of unusual or serial-related crimes like rape or murder, because it focuses on the evidence at the crime scene, the general background details of victims and development of physical background of offenders. Krause (2007: 28) emphasises that it is aimed at understanding the behaviour and psychological wellbeing of offenders involved in the crime. Geographic profiling to determine crime locations, identify the residential address of offenders and prioritise such areas assist the police immensely in apprehending offenders (Santos, 2013: 60). According to the researcher investigative crime analysis could help investigators to trace both offenders and victims through recovery and analysis of cybercrime evidence, as well as the gathering of information related to cybercrime activities to ensure that reliable and valid evidence is presented to court.

5.3.6 Intelligence crime analysis

Intelligence crime analysis is mostly applied in situations that involve organised crime activities to link people, events and property to certain occurrences. According to Hill and Paynich (2014: 10), this analysis can be used through surveillance, informants, and undercover operations as well as other sources of information such as telephone records, travel information, bank statements, tax records and business associates of suspects that are involved in the same criminal activities. It analyses the entire criminal enterprise to understand how syndicates are linked to business deals, who are the role players and the leaders of these syndicates. Krause (2007: 28) opines that the aim of intelligence analysis is to collect, evaluate, analyse, integrate and disseminate information relating to criminal organisations and their associates to identify criminal activities. Is used to support police in the crime investigation processes by digging deeper into the investigated crime to identify crime threats in detail to understand its root causes and identify crime patterns and trends to recognize the behavioural characteristics of offenders (Berning & Masiloane, 2012: 86). Santos (2013: 60) points out that this helps the police to intervene and apprehend criminals such as those involved in human trafficking, weapon trafficking, cybercrime rings and cash in-transit

robberies. The researcher is of the view that intelligence crime analysis can also help police to combat organised crime such as cybercrime, support them in the criminal investigations, preservation and presentation of cybercrime evidence.

5.4 THE CRIME ANALYSIS PROCESS TO COMBAT CYBERCRIME

The crime analysis process consists of both qualitative and quantitative data analytical techniques that can help the police in combating crime (Mashiloane, 2014: 128). Qualitative data and an analytical technique involve non-numerical data for examination, interpretation and observation of the phenomenon in the natural settings to detect underlying meaning and patterns of the relationship. For example, it includes crime reports such as victim statements, witness statements and crime information that are contained in police dockets as a form of qualitative data. Crime analysts use crime analysis techniques to dissect these statements and crime information to establish past relationships.

Quantitative data and analytical technique use manipulation of observations to describe and explain the phenomena that emanate from observations that use statistical methods (Boba, 2001: 9). Crime analysts use analysis techniques to analyse crime information like the date and time of occurrence, the location of crime and crime types using statistical methods to analyse these variables (Mashiloane, 2014:129). Santos (2013: 53) states that the crime analysis process entails steps such as collection, collation, analysis, dissemination and feedback to address the crime. The first step in the crime analysis process is gathering and collection of crime information, the second step is to sort, extract and store crime information, the third step involves analysis of gathered and collected crime information, the fourth step is to share the findings with other crime analysts, and the fifth step is to evaluate results from crime analysts to ensure validity and reliability of crime information (Stering, 2008: 51). The crime analysis process needs to be followed from the beginning of the analysis process to the end to achieve the objective steps of the crime analysis process. According to Matsaung (2019: 42), this helps crime analysts to provide the police with useful crime information to investigate crime, trace and identify suspects who will be successfully prosecuted.

Data collection: Data collection is a process in which crime analysts gather and collect crime information by pulling together various sources on a daily basis during the police operation (Newburn, 2003: 342). Crime analysts can receive crime information from different sources both internal and external. Internal sources comprise crime reports on police dockets, crime reports from crime intelligence, undercover police agents and police informants. External sources include crime information on electronic media, social network platforms, other law enforcement agencies and government departments (Mashiloane, 2014: 129-130). Regarding cybercrime, investigators collect crime information such as the identities of cybercriminals, their organisations, and modus operandi to target victims.

Data collation: Data collation is a process of organising crime information into categories and subcategories. This means that crime analysts will categorise and classify crime information from various sources such as police crime reports, media reports and reports from other law enforcement agencies. According to Osborne and Wernicke (2003: 31-32), crime analysts categorise crime reports at this stage by making folders for residential burglary reports, robbery reports, auto thefts etc. The categorisation of the received reports is done before crime analysis can take place (Stering, 2008: 510). The researcher believes that data collation can be used for any information collected on criminal activities and that will include relevant information collected on cybercrime as well.

Analysis: Analysis is one of the important steps in crime analysis process. Crime analysts examine and process data and turn it into packages of information that can be used on crime series, patterns and trends (Stenton, 2006: 19). The role of crime analysts at this stage is to interpret and provide meaning that can be used by police management, visible policing and detectives to reduce crime through collected data to achieve policing objectives (Mashiloane, 2014: 131). Analysis generates intelligence that helps crime analysts to understand and explain crime problems on hand and to interpret intelligence to know what causes the crime (Mashiloane, 2014: 157). It assists the police with accurate information that can be used in crime prevention, investigation of crime and apprehension of criminals (Horne, 2009: 71). Osborne and Wernicke (2003: 33) emphasise this by stating that analysis is the core step in which crime analysts turn the collected information into intelligence that is disseminated and can

be used for crime prevention or combating activities. In the context of this study, analysis helps the police to determine the modus operandi of cybercriminals and the digital platforms that they target.

Dissemination: Dissemination is the stage in which the final product of crime information is packaged and circulated to the users who need to use it for crime prevention, crime combating and crime investigation (Govender, 2012: 86). The outcome of analysis reports is released to the police for utilization based on conditions and protocols of observing security classification of the information and security clearance of the client. Govender (2011: 124) states that dissemination can be done through various means such as workshops, reports, face- to- face sessions or via various media platforms. It could also be done by means of crime bulletins such as administrative and tactical reports (Osborne & Wernicke, 2003: 36). It supports the police towards crime prevention, sharing information about criminal activities and disorder problems and can also be used during daily police operational activities (Santos, 2013: 58). It will also entail disseminating intelligence on cybercrime incidents that could be used in the prevention, investigation and arresting of cybercriminals.

Feedback: Feedback is the last step of the crime analysis process and a crucial analysis process which requires refinement and advancement of crime analysis (Stenton, 2006: 24). Feedback is an outcome derived from the analytical process which necessitates modification and improvement of the analysis process. This step can improve the quality of the analysis, the value of data that was used and the usefulness of the analysis process in decision making. Feedback is also a tool that helps analysts to improve the analysis process in order to modify their procedures and refine their methods to ensure that the analytical process is continually improved (Mashiloane, 2014: 133). Govender (2012: 87) affirms that feedback emanates from the users of intelligence to report back to crime analysts, thus informing them about the outcome of the crime analysis product. Crime analysts consequently learn which end products of crime analysis work or do not work to ensure that analysts take note on how best users plan to use analytical products as well as the value of implementing end results of analysis in combating crime (Govender, 2011: 125). In the context of this study, feedback from analysis could indicate how the information was used and the type of information that is useful in the policing of cybercrime.

5.5 THE PROCESS OF INVESTIGATION OF CYBERCRIME

The South African Police Service is mandated by the Constitution of the Republic of South Africa of 1996 and the South African Police Service Act 68 of 1995 to investigate crime, thus empowering the police to collect crime-related information that will assist them to prevent, combat and investigate crime. Ezeji (2014: 73) states that the police collect crime information, question both victims and witnesses, re-construct the crime scene, prepare case dockets, trace suspects and prepare the case docket that is handed to the National Prosecuting Authority for prosecution. The above-mentioned summarises the process of criminal investigation where evidence is gathered in order to prosecute offenders. Criminal investigators use this process to identify crime scenes, suspects and victims, gather evidence, arrest criminals, recover what was stolen or robbed during that incident and bring criminals to court (Thenga, 2018: 99). The exponential increase of cybercrime worldwide overwhelms investigators and the researcher is of the view that cybercrime investigators should be aware that crime could take many forms as it could be committed through emails, instant messages, and software programmes. Ezeji et al. (2018: 101) assert that during the commission of cybercrime, criminals may hide their identity and use other peoples' identities in order to gather information about the victims, share information with other cybercriminals and coordinate meetings with their associates with the intention of launching an attack.

During the investigation process, cybercrime investigators should strictly follow investigative principles and procedures when collecting and retrieving evidence. According to Ezeji (2014: 71), this will ensure that investigators are thorough because computer or electric devices can store large amounts of information that may be inter-linked with other crimes that occur in cyberspace. The correct investigative procedures must also be adhered to during the recovery and collection of computer evidence. No changes should be made to the evidence found at the crime scene, and the necessary precautions must be taken while gathering evidence to avoid alterations. Evidence must be photographed before it is examined and computer forensic expert must testify to the validity and integrity of evidence (Mandia, 2011: 42). The investigators of cybercrime must at all times handle digital evidence with care and safe keep it in lockable evidence rooms because if the evidence is tampered with, it becomes

inadmissible in court. Therefore, the evidence found at a crime scene must be preserved until it is handed over to a computer forensic expert for scientific analysis and the court to serve as proof (Ezeji, 2014: 73). The collected evidence is an important tool that can be used to direct investigators in the identification of suspects and linking them to crime and apprehending them based on their online criminal activities. The investigators can use computer evidence combined with traditional investigation techniques to help in identifying, tracing, allocating and arresting cybercriminals (Ezeji, 2014: 75).

The main challenge in the investigation of cybercrime is that the information that might be required to prove cybercrime activities such as the computers of both victims and suspects might be in different countries and not easily available to the investigators in the country where this crime has been committed. That is why Kopelev (2000: 60) states that cybercrime requires investigators who are highly trained in cybercrime investigation to ensure effective and efficient investigation. This situation warrants the appointment of investigators who are knowledgeable about computer software and skilled in the investigation of cybercrime to identify the required evidence and be able to interpret it to enhance successful investigation. However, Ezeji (2014: 71) accentuates the importance of investigators who have initiated the investigation to remain in the investigation throughout the entire process to assist in directing the investigation even though deviations may occur due to unforeseen circumstances.

5.6 THE CHALLENGES IN THE INVESTIGATION OF CYBERCRIME

The increased access to and use of technology for daily activities expedite the increase in cybercrime because it is also accessed by people with criminal intentions. Its borderless nature enhances its complexity and poses a challenge for its effective and efficient investigation because it largely depends on the effective cooperation of various law enforcement agencies across multiple jurisdictions. According to Urbas (2012: NP), this requires law enforcement agencies where cybercrime occurs to have formal and informal communication channels to enhance cooperation that will ensure the sharing of information as well as joint investigations. The use of anti-forensic Tactics, Techniques and Procedures by cybercriminals compound this further. According to Mngadi (2021: 21-22), it makes it difficult for digital forensic investigators to compile enough digital evidence because certain data on the computer or electronic

devices may be hidden or deleted, thus compromising the investigation process and bringing into question the validity of the investigation.

The borderless nature of cybercrime makes its policing costly because it demands cooperation and cross-border travels that requires a steep budget that might require investigators to travel across countries to collect evidence. This requires much investment and commitment by law enforcement agencies around the globe to ensure that funds are available to deal with this crime efficiently and effectively (Dlamini & Mbambo, 2019a: 7). The increase of this crime signifies the challenges in policing it as indicated by Mngadi (2021: 20) because it is growing at an alarming rate.

According to Kader and Minnaar (2015: 71-72), the difficulty of investigating and prosecuting cybercrime indicates the challenges faced by law enforcement agencies around the world. The technical aspects and procedures in the investigation of cybercrime is still at the development stage to respond to the developing and changing cybercrime environment as well as understanding the modus operandi of cybercriminals (Mngadi, 2021: 21). As a result of the increasing nature of cybercrime worldwide, it is even questionable whether the police do launch an investigation on reported cybercrime incidents and locate offenders. According to Edward (2019: 2), police resources are overburdened with various tasks and there are very few skilled cybercrime investigators who always have more work than they can handle. Irons and Ophoff (2016: 275) point out that these challenges could be addressed through developing a strategy that checks cyber threats by observing and analysing cybercrime reports to help cybercrime investigators to obtain relevant knowledge on the tactics of cybercriminals.

5.7 THE ROLE OF INTELLIGENCE-LED POLICING IN THE INVESTIGATION OF CYBERCRIME

Intelligence-Led Policing plays an important role in the investigation of cybercrime by focusing on criminal activities. This means that Intelligence-Led Policing can be used to identify the problem and quantify them by intelligence assessment and subsequently targeting criminals for investigation and prosecution (Myeza, 2019: 116). Intelligence-Led Policing is used in crime investigation to aid the police to arrest most persistent and prolific offenders that cause disorder in the community (Ezeji, 2017:

245). Ezeji (2017: 246) emphasizes that this model can be used in crime investigation by employing a command-driven process that targets prolific offenders for identification, arrest and prosecution based on the risk assessment of the harm that is caused in the community. This should be underpinned by the core principles of Intelligence-Led Policing to collect data effectively and understand crime hot spots, the location where crime occurs and the people who are involved in criminal activities, thus arresting them to enhance deterrence (Hartfied & Kwewen, 2008: 9).

Intelligence-Led Policing advocates the use of an E-docket system which purpose is to assist in the management of dockets within policing. The E-docket system captures all information related to crime investigation, while the manager of the investigation team has access to this system to be able to track the process of the investigation and the work that is done on the docket on the system (Ezeji, 2017: 245). The E-docket system also provides for instant message communication to communicate with victims by alerting them about the process of the investigation. This system can also help managers to send instant messages to investigators to instruct them to speed up the investigation (Decock, 2004: 55). The E-docket system would be expedient in transferring dockets and thus facilitating the investigation of cybercrime.

5.8 THE ROLE OF THE CRIMINAL JUSTICE SYSTEM IN COMBATING CYBERCRIME

The role of the criminal justice system relates to the process in which justice handles the victims, suspects and societies in accordance to the law (Ezeji, 2017: 287). The criminal justice system consists of four major role players which are the police, the National Prosecuting Authority, the court and correctional services. The police are responsible for crime prevention, crime combating and crime investigation; the National Prosecuting Authority prosecutes accused persons; the courts adjudicate on the guilt or innocence of accused persons; and Correctional Services have to rehabilitate convicted offenders. The roles of these agencies are to ensure that social harm is prevented through apprehending violators of the law, punishing them by enforcing the law, thereby deterring potential criminals from violating the law (Thenga, 2018: 91). An effective criminal justice system ensures that offenders of cybercrime are apprehended, convicted and sentenced. It is necessary that police and other stakeholders in the criminal justice system guarantee that the society will trust the

system to report cybercrime- related activities without fear (Ezeji et al., 2018: 102). Kader and Minnaar (2015: 74) stress that the reporting mechanism must always link with the police cybercrime consumer awareness and education programme to inform society about the risk associated with cybercrime and encourage them to report cybercrime- related activities.

5.9 THE THEORIES OF PUNISHMENT

Punishment is an intentional action taken by lawmakers to cause pain to the offenders and it may be physical or non-physical. The role of punishment is to humiliate offenders who violate the law of the country by inflicting punishment that is balanced to the harm caused to prevent them from committing further crimes. During punishment offenders might undergo rehabilitation for correcting their criminal behaviour (Thenga, 2018: 94). The role of punishment is the infliction of pain to offenders as a penalty for crimes that are regarded as harmful to the entire society (Muthapuli, 2012: 68). According to Muthapuli (2012: 69), punishment is pain or any other consequence that is considered to be unpleasant to the offender and is imposed by those who possess legal authority over the offender for the implementation of the law. According to Thenga (2018: 94), there are three theories of punishment, which are retribution, deterrence and rehabilitation.

5.9.1 Retribution theory

Retribution is based on the principle that wrongdoers should be punished as consequences of crime because they deserve it. Retribution theory focuses on the principle that offenders who commit crime disturb the balance of the legal order that can only be restored if the offenders are punished (Muthapuli, 2012: 71). The main objective of retribution is that offenders who committed crimes should be punished so that they could comply with the laws of the country. This theory is based on seeking revenge and it complies with the Biblical principle of 'an eye for an eye'. However, the Biblical principle of 'an eye for an eye' cannot be applied in South Africa as it will violate the constitution (Thenga, 2012: 95). Sentencing is regarded as retribution and is designed as punishment for crimes committed, and it is seeking revenge even if is difficult to determine what punishment will be equal to the harm caused. Retribution emphasizes that punishment must automatically follow after the crime has been committed as it reflects the community's condemnation of crime (Thenga, 2012: 95).

The principle of retribution is not only applied to offenders to reconcile with laws of the country by undergoing punishment, but is also seen as a reflection of the community's condemnation of the crime. Retribution is based on the fact that if the offender is not punished, he/she could commit further crimes which may cause negative consequences to members of the community, because those who are directly affected by the crimes, may take the law into their own hands as revenge (Muthapuli, 2012: 71). Based on the understanding of this theory, the offenders of cybercrime must be punished to prevent them from committing further cybercrimes.

5.9.2 Deterrence theory

Deterrence is punishing an offender to prevent future criminal behaviour and the outcome of punishment should serve as deterrent to the offender and other potential offenders who are planning to commit crime. It is based on the crime control strategy that uses punishment to deter the offender and other potential offenders to commit crime. According to Labane (2012: 29), this theory sets an example to potential offenders to be aware of the consequences of crime as the punishment that is imposed to those offenders involved in criminal activities will indicate to others what will happen to them should they commit crime. Thenga (2012: 96) reiterates this by stating that the essence of deterrence is to show individuals that harsh sentences are imposed on offenders and the same will apply to them should they be involved in similar criminal activities (Thenga, 2012: 96).

There are two types of deterrence – namely, special deterrence and general deterrence. Special deterrence affects offenders that are already punished for the crime they had committed and punishment forces them to stop engaging from any criminal activities in future. The underlying principle of special deterrence is that offenders who experience the pain and unpleasantness of punishment will stay away from committing crime in future (Du Preez & Muthaphuli, 2019: 36). On the other hand, general deterrence applies to any individuals other than offenders who are already punished to avoid engaging in criminal activities because they are afraid of actions that might be imposed on them should they be apprehended. The principle of general deterrence is to use punishment against apprehended offenders as example to show other individuals in the community the consequences of engaging in criminal activities.

General deterrence can help members of the community to comply with the law and refrain from committing crime because they are afraid that if they might be caught, they will receive severe punishment (Du Preez & Muthaphuli, 2019: 36). The researcher's view is that deterrence is a punishment that could be used against cybercriminals to deter them from committing cybercrime in future. Deterrence can also be used as example to show other potential cybercriminals that engaging in cybercrime activities will lead to severe punishment.

5.9.3 Rehabilitation theory

Rehabilitation is a programme of corrections that is provided to convicted offenders to promote educational, vocational and life skills training to change their criminal behaviour and to assist to integrate them into community as law abiding citizens (Champion, 2001: 17). Rehabilitation plays an important role for correcting offending behaviour, to promote human development and social responsibility of offenders. It helps offenders to understand what impact their crime has had on the victims whereby offenders can change their criminal attitudes, behaviour and social circumstances (Jonker, 2011: 38). Rehabilitation promotes positive values and responsibility for criminals, helps to prevent recidivism and focuses on a holistic approach through multi-disciplinary teams to address the causes of criminal behaviour and empower them with skills development to integrate successfully back into communities (Jonker, 2011: 38). It is a process that requires offenders to come to the realisation that their criminal behaviour caused harm to the victims, acknowledging their mistakes and showing remorse as a positive attitude to turn around and change to become law-abiding citizens. However, offenders must understand that rehabilitation is an ongoing process and not a once-off event because it requires offenders to discover the truth about themselves and acknowledge the reality of life (Ezeji, 2014: 96). It breaks the cycle of crime by affording offenders a second chance in life to live with others and be economically active once again (Thenga, 2018: 97).

According to the White Paper in Corrections in South Africa (2005: 36), rehabilitation consists of the following aspects:

- Offenders accepting the responsibility of their crime and be accountable for their actions;
- Separating the offender from the offending behaviour;

- Changing criminal attitudes and social circumstances to address criminality;
- Promoting positive values and responsibilities on offender;
- Ensuring that causes of criminal behaviour are addressed;
- Ensuring that recidivism is prevented as far as possible;
- Ensuring that structured programmes are provided to empowering offender skills development and vocational training;
- Conducting needs and risk assessment analysis on offenders; and
- Ensuring that offenders are successfully integrated back into the communities.

The researcher regards rehabilitation as one of the measures that could help cybercriminals to change offending behaviour.

5.10 CONCLUSION

The efficient and effective use of crime analysis in policing to deal with cybercrime can help the police by providing them with cybercrime information to identify and understand cybercrime threats, provide warning of cybercrime threats on time and address cybercrime threats within communities. Crime analysis is used in policing to combat cybercrime as it helps the police to understand the patterns, series and linkages of various cybercrime activities. It can also help in the monitoring, risk assessment and evaluation to deal effectively with cybercrime threats. Intelligence-Led Policing is an effective crime prevention initiative in policing that is used to deal with cybercrime threats to identify prolific offenders, monitor crime hot spots, collect more data regarding cybercrime activities and is helpful in investigating cybercrime.

It is crucial that cybercrime investigators be trained to possess cybercrime or computer skills as far as possible before they can be involved in any investigation that involves computer or electronic devices to enable them to understand the modus operandi of cybercriminals. Such training can help cybercrime investigators to have knowledge and skills of collecting, retrieving and packaging of computer evidence to aid successful investigation. The criminal justice system plays an important role in combating cybercrime activities through police arresting offenders of cybercrime and bringing them before the court for prosecution and sentencing.

CHAPTER SIX: RESEARCH METHODOLOGY

6.1 INTRODUCTION

Research is an investigation to explore what is not known, identifying knowledge gaps and what is already known about a specific issue (Kumar, 2011: 23). Its main purpose is to produce knowledge, to identify research problems and to address them (Blaikie & Priest, 2019: 43). Research is a value system of individuals and sets expectations of the communal world to inquire about certain topics of the study to know more about their beliefs in that world (Punch, 2016: 175). The purpose of research is collecting, analysing and understanding information of a particular phenomenon of the study (Leedy & Ormrod, 2015: 152). Research is the process that applies to a study in which scientific methods are used to acquire knowledge of the topic of the study. Law enforcement agencies globally use research as fundamental strategy to understand crime problems their respective countries face. Therefore, through research, law enforcement agencies around the world can empower and skill law enforcement officials and develop law enforcement agencies into professional entities (Matsaung, 2019: 66).

In the South African context, the SAPS have a component of research, the role of which is to deal with and manage research within policing to ensure that individuals, organisations, companies and universities who wish to conduct research within the SAPS apply through it to be granted permission before research can be conducted (Matsaung, 2019: 66). The role of the researcher in the study involves the accumulation of information scrutinising it to explain the phenomenon (Creswell, 2014: 247). The purpose of this study is to determine the use of Intelligence-Led Policing in dealing with cybercrime in South Africa and a phenomenological research design was applied. This chapter focuses on the research design, description of the population and sampling method, data collection, data analysis techniques, trustworthiness of the study and ethical issues.

6.2 RESEARCH METHODOLOGY

Research methodology is a process that uses the philosophical premises of the study including research processes, research strategies and data collection methods to address research questions, research objectives and the problem statement of the

study (De Vos et al., 2012: 64). It integrates the research approach, investigation of the study, population, sampling and data collection (Bless, Higson-Smith & Sithole 2013: 380). Kumar (2014: 84) shares the same sentiment by outlining that research methodology is a process that unfolds the research design and the approach that the researcher used. Clough and Nutbrown (2012: 21) state that research methodology applies to different perspectives depending on the researcher's interpretations of the same data; which according to Bless et al. (2013: 63), articulate research design and approach that are relevant to the research study to ensure that the research processes, methods and strategies are applied correctly to achieve the objectives of the research study.

6.3 RESEARCH DESIGN

Research design is a blueprint that gives the researcher a direction on the study (Creswell, 2009: 3). It is a research procedure that needs to be adhered to, which guides the researcher on the entire research study such as the data collection and data analysis processes (Babbie & Mouton, 2012: 74). Similarly, Franklin (2012: 54) explains it as a process that provides an overarching structure of research, the research plan and outlines the research procedure, including the entire process of data collection and analysis. This means that research design provides a detailed investigation and research plan to give the researcher direction how data should be collected and analysed to achieve the objectives of the study as expected. According to Kumar (2005: 84), research design is a road map used by researchers during the research process to find answers to the research question and it involves strategies, structures and plans used by researchers to address the research problem. Creswell (2014: 3) asserts that research design is a detailed plan and the procedure of the study that require researchers to follow research steps from broad assumptions to detailed methods of data collection, analysis and interpretation.

The researcher adopted a phenomenological research design. According to Leedy and Ormrod (2001: 153), a phenomenological study aims to understand the participants' perceptions of and perspectives on the matter being studied as well as meanings that are attached to such. De Vos, Strydom, Fouche and Delport, (2005: 270) explain that the aim of a phenomenological research design is to provide the meaning behind the viewpoints of the research participants regarding the experiences

of the problem at hand. Denscombe (2007:79) indicates that the researcher who uses a phenomenological research design in order to gather new information that has not undergone analysis processes, gives research participants' ideas and reasoning honestly, gather different responses on the research problem based on how research participants' think of social reality depending on present situations that influence their experiences. Some disadvantages of the phenomenological research design are that it may be as difficult for the researcher to be objective or not to be influenced by his/her preconceived responses of problem being studied. Secondly, it may be difficult for the researcher to ascertain if the research participants are telling the truth or not (Denscombe (2007: 86). The researcher used a phenomenological research design to obtain data from research participants by means of one-on-one interviews with crime intelligence members, detective members and the members of the Directorate for Priority Crime Investigation who have experience and knowledge about the use of Intelligence-Led Policing in combating cybercrime in South Africa.

6.4 RESEARCH METHODS

A research method is the strategy that is used by the researcher during the research journey to integrate and manage the research problem that was investigated together with the aims, research questions, objectives, data collection and analysis (De Vos, Strydom, Fouche & Delport, 2012: 66). According to De Vos, Strydom, Fouche and Delport (2011: 63), there are two well-known research approaches, namely - the qualitative and quantitative approaches. A combination of these two approaches is a mixed method research approach. A quantitative approach uses a mathematically-based method for collecting data such as statistical correlations for hypothesis testing (Walliman, 2016: 33). Pattern and Newhart (2018: 22) state that quantitative researchers use deductive methods to plan the research. In a quantitative approach the researcher uses questionnaires and survey questions to collect data from participants (Davies & Hughes, 2014: 149). It also uses a mathematically- based approach for testing existing theories, examining relationships among variables and measure variables by using statistical instruments (Creswell & Creswell, 2018: 4).

In contrast, a qualitative research approach is an investigation of social or human problems in a natural setting to understand the meaning of events or phenomena of the participants. Qualitative researchers use inductive planning for formulating

research questions that are not yet identified (Pattern & Newhart, 2018: 22). The purpose of qualitative research approach is to ask questions to research participants to understand their perspective on the complex nature of the phenomena (Des Vos et al., 2011: 64). Based on the need of this study to explore the use of Intelligence-Led Policing in combating cybercrime, a qualitative research approach was used.

6.4.1 Research Approach

In this study, the researcher used a qualitative research approach to answer the research question and to achieve the objectives of the study. According to Davies and Hughes (2014: 09), a qualitative researcher visits research sites to interview research participants, take field notes, examine documents and record conversations to understand the research problem better. Lanier and Briggs (2014: 14) explain that a qualitative research approach focuses on collecting data and make conclusions regarding responses to the research questions to assist the researcher to achieve the aims and objectives of the study in question.

Qualitative research helps the researcher to understand the experiences of other people about particular events in their lives and interpret them as deemed necessary for the purpose of this research based on its explorative nature. Withrow (2014:298) indicates that a qualitative research approach is based on encapsulating the research processes with the aim of understanding the entire picture of human behaviour to comprehend its meaning and motivation. Creswell (2014:175) points out that the role of a qualitative researcher is to interact with research participants to collect data face to face or through one-on-one interviews on the research problem being studied. As indicated above, in this study the researcher utilized qualitative phenomenology to understand the use of Intelligence-Led Policing to combat cybercrime in South Africa.

6.4.2 Population and Sampling Methods

A research population refers to a group of people from which the researcher hopes to draw a representative sample with homogeneous qualities like those of the total population (Leedy & Ormrod, 2014: 294). Taherdoost (2016: 17) states that it is an entire set of cases that can be used to choose a sample from, thereby supporting the assertion of Welman et al. (2005: 52) that population contains an entire collection of all components of the study from which the researcher is to draw the conclusions.

Population is an aggregate of elements from which the researcher selects a sample (Babbie & Mouton, 2010: 174). It is a total group of people whom the researcher is interested to study (Guthrie, 2010: 68). Such a group can include individuals, groups and settings that the researcher is interested to study (De Vos et al., 2011:391). Punch (2005: 101) emphasises that the population involves the entire group of people who could participate in the study from which the required data could be collected. The population of this study comprises members of crime intelligence, detective services and the Directorate for Priority Crime Investigation in the South African Police Service in selected provinces.

Sampling on the other hand refers to the sub-elements of the population that are selected as the participants in the study (De Vos et al., 2012:79). Punch (2016: 176) emphasises this by stating that sampling is a small portion of a group that is under the study and it is drawn from the population from which data is collected and evaluated. It is a small portion that is selected by the researcher from the entire population (May (2011:93). It gives the researcher a manageable number to work with. Guthrie (2010: 53) defines it as sub-elements of the population that the researcher has selected from the entire population. It is a researcher's strategy to choose the persons interested to take part in the investigation (Fraenkel, Wallen & Hyun, 2015: 107). Terre Blanche, Durrheim and Painter (2006: 565) are of a similar view that sampling is the criterion used by the researcher to select participants from the entire population. The selected sample of this study were members of the South African Police Service in five provinces, namely - Limpopo, Gauteng, Mpumalanga, Free State and North-West provinces who are knowledgeable in the use of Intelligence-Led Policing to combat cybercrime in South Africa.

The researcher used a purposive sampling method in order to get experienced and knowledgeable police officers who were able to assist in answering the research question and achieving the research objectives of this study. According to Gray (2018: 215), in purposive sampling the researcher chooses research participants that would provide rich information to achieve the objectives of the study. De Vos et al. (2011: 392) state that purposive sampling is known as judgemental sampling and it represents the characteristics and attributes of the identified population to achieve the purpose of the study. Bless et al. (2013: 172) emphasise that it is the researcher's

decision to choose a sample and to use application of inclusion criteria as to who could be selected to provide data- rich information to achieve the objectives of the study. Fraenkel et al. (2015: 101) elaborate on this by stating that it is the researcher's decision to choose participants purposefully that he/she trusts who could provide more data about the subject and enable the study to achieve its objectives. In this study the researcher selected research participants based on their knowledge, work experience, rank position and qualifications. The inclusion criteria in this case were police officers who have been dealing with cybercrimes for more than eight years; holding the rank position of Warrant Officers to Brigadiers; with Bachelor Degrees to Masters Degrees in Criminal Justice.

6.5 PILOT STUDY

A pilot study is described as a mini version of the study to outline a full-scale study or a trial preparation of the complete study (Strydom, 2011: 237). It entails the testing of the data collection instruments and their variables. A pilot study helps the researcher to understand and identify unclear interview questions contained in the interview schedule. According to Barker (2003: 327), the researcher develops interview questions after pre-testing interview questions on non-research participants identified with similar characteristics of the research participants in the sample of the study. The main purpose of the pilot study is to test interview questions to identified participants to discover the background and knowledge of the participants of the particular study (Welman & Kruger, 2001: 141). The researcher pre-tested the interview schedule by emailing questions to participants. They were first phoned by the researcher before the questions were e-mailed to them and they all responded to the e-mailed questions. The participants who were chosen to participate in the pilot study were excluded from the main study. Pilot participants were from Limpopo, Gauteng, Free State, North-West and Mpumalanga, comprised one member from crime intelligence, one member from detective services and one member from the Directorate for Priority Crime Investigation and they all responded to the questions.

6.6 DATA COLLECTION

Data collection involves the methods used to collect data such as interviews and a literature review (Creswell, 2014: 189). It is a process of gathering data through interviewing research participants, reviewing literature such as books, journal articles

and government policy documents (Mills & Birks, 2014: 257). Data collection is based on obtaining information that is relevant to the study to assist the researcher to arrive at the solution to resolve the research problem, to achieve the aim and objectives of the study, and to respond to the research questions of the study (Flick, 2014: 33). The researcher used multiple sources to collect the data for this study. According to Leedy and Ormrod (2013: 151), multiple sources of data collection involve interviews, books, journal articles, dissertations or theses and audio-visual materials to help the researcher to address the research problem and achieve the research objectives of the study. In this study the researcher used those multiple sources to explore the use of Intelligence-Led Policing to combat cybercrime in South Africa.

6.6.1 Interviews

Interviews involve a process of collecting data by creating conversation between the researcher and participants or a specific topic or range of topics. According to May (2011: 120), it is a process used by the researcher to understand people's experiences, opinions, feelings and attitudes about the topic that is being studied (May, 2011: 120). Qualitative researchers mostly rely on interviews to collect data from research participants (Marshall & Rossman, 2011: 142). Interviews as a data collection strategy constitute primary sources to obtain first-hand information from the research participants with the aim to help the researcher to address the research problem and to answer research questions (Leedy & Ormrod, 2013: 97). According to Flick (2011: 107), the researcher conducts in-depth interviews with the research participants, and such interviews should be short, concise and questions that are asked should be clear.

In this study, the researcher used semi-structured interviews. The benefit of using this interview technique is to enable participants to answer questions based on what they know or experienced while focusing on the topic of the study and what the researcher intends to cover (May, 2011:35). The role of semi-structured interviews in one-on one interviews is limited to two people, namely - the researcher and participant (De Vos et al., 2011: 296). According to Bernard (2013: 182), researchers use semi-structured interviews because they allow them to compile an interview schedule that consists of questions that are designed for the specific study. To achieve the objectives of the study, the researcher used semi-structured interviews with research participants. This type of interview involves a limited number of research participants, namely -

participant and researcher. Creswell (2014: 190) explains that when the researcher conducts one-on-one interviews (semi-structured interviews) with research participants, each question of interview schedule is developed to be related to the research topic. Therefore, the questions that were posed during the interview were designed to ensure that the problem being studied was clearly understood.

The data saturation approach was used to determine the sufficiency of the information collected from these participants. According to Bless et al. (2013: 164), data saturation means that the researcher would collect data until no more new information emanates from the participants, but they are merely repeating what has been covered by previous participants. In this study, the researcher stopped interviews after interviewing three more participants who repeated what had already been covered by other participants, meaning there three extra people were interviewed beyond the saturation point. In respect of this study, a total number of 160 people interviewed and the saturation points were researched as follows:

- In Limpopo 12 detectives were interviewed and saturation point was reached at number 09, an extra three detectives were interviewed beyond the saturation point.
- In Gauteng 11 detectives were interviewed, saturation point was reached at number 08 and an extra three detectives were interviewed beyond the saturation point.
- In Mpumalanga 15 detectives were interviewed and the saturation point was reached at number 12, an extra three detectives were interviewed beyond the saturation point.
- In the Free State 12 detectives were interviewed and the saturation point was reached at number 09, an extra three detectives were interviewed beyond the saturation point.
- In North-West 13 detectives were interviewed and the saturation point was reached at number 10, an extra three detectives were interviewed beyond the saturation point.
- In Limpopo 08 crime intelligence members were interviewed and the saturation point was reached at number 05, an extra three crime intelligence members were interviewed beyond the saturation point.

- In Gauteng 07 crime intelligence members were interviewed and the saturation point was reached at number 04, an extra three crime intelligence members were interviewed beyond the saturation point.
- In Mpumalanga 09 crime intelligence members were interviewed and the saturation point was reached at number 06, an extra three crime intelligence members were interviewed beyond the saturation point.
- In the Free State 08 crime intelligence members were interviewed and the saturation point was reached at number 05, an extra three crime intelligence members were interviewed beyond the saturation point.
- In North-West 11 crime intelligence members were interviewed and the saturation point was reached at number 09, an extra three crime intelligence members were interviewed beyond the saturation point.

- In Limpopo 11 members of the Directorate for Priority Crime Investigations were interviewed and the saturation point was reached at number 08, an extra three crime intelligence members were interviewed beyond the saturation point.
- In Gauteng 13 members of the Directorate for Priority Crime Investigations were interviewed and the saturation point was reached at number 10, extra three crime intelligence members were interviewed beyond the saturation point.

- In Mpumalanga 08 members of the Directorate for Priority Crime Investigations were interviewed and the saturation point was reached at number 05, an extra three crime intelligence members were interviewed beyond the saturation point.
- In the Free State 11 members of the Directorate for Priority Crime Investigations were interviewed and the saturation point was reached at number 08, an extra three crime intelligence members were interviewed beyond the saturation point.
- In North- West 11 members of the Directorate for Priority Crime Investigations were interviewed and the saturation point was reached at number 08, an extra three crime intelligence members were interviewed beyond the saturation point.

The researcher conducted face to face interviews with members of the detective services and the Directorate for Priority Crime Investigations in Limpopo, Gauteng, Mpumalanga, Free State and North- West. Field notes were taken and audio recordings made after obtaining prior consent from the participants. As for the Crime

Intelligence members, the researcher conducted telephonic interviews with participants in Limpopo, Gauteng, Mpumalanga, Free State and North- West. Note-taking and audio recording were also done as in the case with the face-to-face interviews.

Creswell (2014: 193) states that during the interview process the researcher should take field notes and audio recordings with mutual agreement of research participants. For this study, the recordings and the notes shall be kept in a safe place and their confidentiality maintained for a 5 year period, as prescribed by the ethical clearance and be destroyed thereafter.

6.6.2 Literature Review

The literature review helps the researcher to understand the background of the study, identify gaps from the research conducted by other researchers and inform or guide future research. Gray (2018: 98-103) states that it involves the study of peer-reviewed journals, books, conference papers, statistics, monographs, government publications, legal and professional publications on the research topic. According to De Vos et al. (2005: 123), a literature review familiarises the researcher with the topic being researched and helps in the identification of existing literature on the topic to address the identified research problem. It is a strategy for searching academic literature that has already been published by other researchers and experts on a similar subject that is being researched (Fink, 2010: 3). It helps the researcher to understand and make decisions on what to study, depending on the available information about the topic that reveals what has been researched on the subject and from which perspective (Jesson, Matheson & Lacey, 2011: 16). A literature review helps the researcher to have exposure about the subject, familiarise himself/herself with the content of the subject and the trends in the field to compare local and international theories to identify gaps that still exist on the subject (Kumar, 2014: 92). It helps the researcher to network with other scholars who are researching similar topics to enable the researcher to expand the scope of the study and to identify new knowledge that exists on the study to close the gaps (Hesse-Bier & Leavy, 2011: 39).

6.7 DATA ANALYSIS

Data analysis is a process of ordering, structuring and giving meaning to the collected data as well as comparing information from respondents, developing the findings and recommendations to achieve the objectives of the study (Leedy & Ormrod, 2014: 148). Creswell (2013: 180) elaborates on this by stating that data analysis prepares and organises the text data into transcripts and images to reduce data into themes. According to De Vos et al. (2011: 333), once the coding and condensing of codes have been completed, data should show in figures, tables and discussions, which is then used in such a way that the researcher organises, interprets and gives order to a large amount of data. Creswell (2009: 186) states that the Tesch data analysis method is used to analyse textual data systematically. For the purpose of this study, the researcher adopted the following eight steps of the Tesch method that are described in Creswell (2014: 198) and Tesch (1990:142-145):

- Step 1: transcriptions were carefully read to get the sense of ideas.
- Step 2: documents were carefully read to understand the whole idea.
- Step 3: a list of similar topics was made and such topics were grouped together.
- Step 4: similar topics were named.
- Step 5: similar topics belonging to the same category were grouped together.
- Step 6: each category was marked by name and arranged in alphabetical order.
- Step 7: data material belonging to the same category was organised, grouped together and preliminary analysis was done.
- Step 8: existing data was recorded.

6.8 VALIDITY AND RELIABILITY OF THE STUDY

To ensure validity, the research instrument should measure what is supposed to measure (Gray, 2018: 152). Validity means that data collected by the researcher should reflect the truth and originality of findings presented by participants (Babbie & Mouton, 2010: 122). According to Creswell and Clark (2018: 217), validity of the study is based on checking whether the data collected from participants is accurate and the extent of the credibility, transferability, dependability and confirmability of the collected information has been achieved. As indicated in section 6.6 above, the researcher used various sources of information to build coherent justification for the findings. Creswell (2014: 201) states that if the findings of the study are established through converging

of various sources of information or several viewpoints of participants then that confirm validity. To ensure the validity of this study, the researcher ensured that the information provided by the participants was accurately documented, recorded, analysed and findings accurately presented.

Reliability on the other hand, means that during the research process, every step taken to collect data produces the same results when repeated. It means that measuring instruments used to measure a certain phenomenon produce the same results every time the measurement methods are repeated (Babbie & Mouton, 2010: 119). Gray (2018: 155) calls that the stability and consistency of the research findings. Its main purpose is to ensure that when research findings are measured under the same conditions, in different places and times they should produce the same scores (Punch, 2005:95). In this study, the researcher used member checking to ensure reliability. According to Marshall and Rossman (2011: 42), member checking involves inviting the participants to confirm the findings of other participants to ensure reliability. According to Creswell (2013: 251), member checking is applied when the researcher scrutinises the correctness of the research findings by accepting the results of the findings and giving the participants a chance to verify the truthfulness of the research findings. Bryman (2012: 46) shares the same view with Creswell (2013: 251) by arguing that member checking is when the researcher engages with the research participants by comparing the preliminary research findings and final research findings to reflect on the accurateness of research findings to understand the participants' true version of the verbal communication during the process of empirical data collection. As previously indicated, the researcher interviewed members of crime intelligence, members of the detective service and members of the Directorate for Priority Crime Investigation who deal specifically with the use of Intelligence-Led Policing to combat cybercrime in South Africa

6.9 METHODS TO ENSURE TRUSTWORTHINESS OF THE STUDY

The validity and reliability of the study should be tested to ensure its trustworthiness. Validity means that the outcomes of the study should reflect the true originality of the data. On the other hand, reliability means that if the same steps are followed to obtain data during the research process, the same results would be produced (Babbie & Mouton, 2010: 119-122). The researcher adopted the approaches developed by Bless

et al. (2013: 236-237), namely- credibility, dependability, transferability and conformability to ensure the trustworthiness of the study. The researcher indicates to the readers how the results were obtained and followed each step of the research process to indicate that the results obtained reflect the context of the original sources.

6.9.1 Credibility

Credibility relates to the trustworthiness of the study through openness and good characteristics of the research study that affects the originality of the research findings. Tracy (2013: 248) states that credibility entails that participants and readers of the research study understand the lived experiences described by the research. It entails that the findings of the study should be evaluated and believable from the participants' point of view as the sources of information emanate from them and their information is converted into the findings of the study (Kumar, 2014: 219). Credibility means that the data obtained makes sense to the reader accessing the study and that the study demonstrates the appropriateness of the research questions, research design, data collection methods and data analysis approaches. The researcher should be in position to defend the research design and methodology used in terms of theory and knowledge about the study. As stated by Creswell (2013: 191), the researcher conducted interviews with participants and repeated the same questions for comparing responses to see whether there were similarities or differences on similar issues.

6.9.2 Dependability

Dependability means that the research findings are stable and consistent at all times during the research processes. It means that the researcher should follow the research process and procedures correctly to ensure that the research is presented logically and documented correctly, making it possible to arrive at the same findings when the entire process is repeated within the similar context with the same participants (Bless et al., 2013: 76). To ensure dependability, the study should precisely describe the research strategy to clearly show the research process followed indicating that each step of the research has been thoroughly completed. Denscombe (2010: NP) states that if the research fails to describe the sampling method in detail, even if the applied sampling method is correct, reviewers will not trust the results obtained from that sampling. This emphasises the need to describe exactly how the findings of the study have been collected, coded and analysed for the study to have dependable outcomes.

To ensure dependability in this study, the researcher recorded interviews with participants and took field notes.

6.9.3 Transferability

Transferability refers to the extent to which the results or the findings of the study can be transferred to other contexts or settings using other participants. It means the readers of the study can determine the applicability of the study to their context (Babbie & Mouton, 2012: 277). For the study to be transferable, it should have a detailed description of the settings, place of research and participants who took part in the study. The detailed description of information involves the qualifications and work experience of the participants. However, transferability provides the steps of research process that were fully detailed about data collection, analysis and the production of the final research report. The research process guides the researcher to replicate the study, to make comparisons, assess the results and evaluate similarities as well as dissimilarities in other settings or contexts (Bless et al., 2013: 104). Transferability is comparing the external validity to show that when the study is applied to other similar contexts, it can produce the same results. It means that the information obtained allows the researcher to compare and assess the similarities between given situations and other contexts. During the research process the theoretical parameters of the research ensure that those who are involved could determine whether or not the theoretical parameters can be generalised and transferred to other settings (De Vos et al., 2011: 346).

6.9.4 Conformability

Conformability entails that if the same research was conducted by different researchers the same results would be obtained. Confirmability designates a repeatable research project and the same results would be produced by other researchers in similar contexts and even if the research was conducted by other researchers the results would be the same (Bless et al., 2013: 237). Conformability means that if another researcher obtained data in a similar situation in different places, the same results could be produced in similar contexts. It allows the reader to understand the purpose of the study, why the study was done in a particular manner and in what context the study was conducted. According to Rolfe (2004: 506), to ensure conformability, the researcher should convince the readers that the results

obtained are verified as true from the original data. Babbie and Mouton (2010: 122) state that to ensure conformability, the researcher must be able to prove that the results of study were obtained by following the research meticulously step- by -step throughout the entire study. The same view is shared by Kumar (2014: 219) who points out that conformability refers to the extent to which the results of the research could be verified by other researchers in respect of compatibility of the findings and the conclusions drawn from them.

6.10 ETHICAL CONSIDERATIONS

Ethics refer to the standard of professional behaviour set to guide researchers on how best to act towards participants during the data collection process (Guthrie, 2010: 15). Ethics include respect for the entire research process, research participants and beneficence, meaning that participants' privacy, anonymity and the right to participate in the study should be respected. The researcher must avoid as far as possible, to use the participants in the study as only the instruments of getting what he/she wants without due regards for their wellbeing. Beneficence means that the researcher should ensure that participants are not harmed by a particular study and their safety remains a priority (Marshall & Rossman, 2011: 47).

Ethics involve a set of principles or norms that show the characteristics of the researcher and guide his/her moral choices and relationships with others. To ensure ethical principles, the researcher should ensure that participants are not harmed by the study and should obtain informed consent that guarantees the privacy, respect and avoids deception (Gray, 2018: 70-75). UNISA's policy on research ethics outlines the responsibility of the researcher in undertaking ethical research and avoids any form of unethical research practice when collecting data (UNISA, 2013: 2). The researcher adopted the following ethical principles, namely - informed consent, confidentiality, anonymity and non-maleficence.

Informed consent - Informed consent means that detailed information about the research is provided to research participants for them to make informed decisions whether to take part in the study or not (Gray, 2018: 76). It is a mutual agreement between participants and the researcher as moral code to be communicated about a particular study so that informed decisions could be made by people who partake in

the study (Leedy & Ormrod, 2013: 392). Harding (2013: 25) states that it entails the judgement of the participants to voluntarily agree to participate in the study and to understand what the research project entails. Creswell (2013: 174) emphasises that the principle of informed consent entails the provision of voluntary formal consent by participants and the provision of full disclosure about the study by the researcher. To ensure informed consent, the researcher provided consent forms to participants before the collection of data to indicate the mutual agreement of their participation in the study.

Confidentiality - Confidentiality means that the information provided by participants should be strictly treated to maintain privacy (Gray, 2018: 79-80). Confidentiality means that the researcher should at all times ensure that private details and information provided by research participants are not circulated to others (Oliver, 2010: 81). It entails that information provided should not be shared without the approval of the participants (De Vos et al., 2011: 61). To ensure confidentiality, the researcher ensured that the identity of the participants is protected.

Anonymity - Anonymity is the protection of the identity of the people who take part in the study to provide information to the researcher (Harding, 2013: 26). According to Bless et al. (2013: 389), anonymity entails the promise by the researcher to the participants that the information that they provide will remain unidentifiable from its source, meaning the researcher should protect the identity of the participants against any risk. Any person who accesses the research report would be unable to identify the person who provided the information (De Vos et al., 2005, 61-62). To adhere to anonymity in this study, the researcher did not reveal the identities of the people who participated in the study.

Non-Maleficence - Non-maleficence means that the physical and psychological harm of the research participants should be protected (Leedy & Ormrod, 2013: 105). It means that the researcher should ensure that no injuries are inflicted on research participants as far as possible (Bless et al., 2013: 29). To ensure non-maleficence, the researcher adopted research ethics to protect participants against any discomfort that may emerge from the study. Unisa's policy on research ethics emphasises that during the research process the researcher should be honest when reporting findings of the

study and refrain from deceiving participants about the purpose of the study (Unisa, 2013: 3-6). For the purpose of this study, non-maleficence is an important principle of research and the researcher conducted research in such way that the risk of harm was avoided, as he respected the rights of individuals and reported the findings honestly.

Ethical considerations also focus on plagiarism and honesty in reporting the results that arise from the research. Universities around the world have ethics committees that enforce ethics codes, approve all research projects undertaken and it is the responsibility of researchers to comply with ethics codes to protect the rights of humans or animals who participate in any study. The researcher obtained ethical clearance from the University of South Africa for conducting this research and the permission from the South African Police Service and the Directorate for Priority Crime Investigation to interview their members.

6.11 CHALLENGES ENCOUNTERED IN THE STUDY

The challenge encountered in the study was the six months delay in obtaining permission to conduct interviews with Detective, Crime Intelligence and Directorate for Priority Crime Investigation members. After the researcher obtained permission to conduct the research within the above mentioned components, another challenge encountered was the continuous change of the interview dates or times with some research participants despite the fact that they agreed in advance for specific dates and times. That warranted constant rescheduling of the meetings and delayed the time that was set by the researcher to complete the interviews. The scheduling and rescheduling of the meetings due to unavailability of some participants led to telephonic interviews with crime intelligence members rather than face-to-face because the researcher had to be at different provinces as per his initial travel schedule. Despite these challenges the researcher managed to interview all the people that he set out to interview, so those challenges did not have a bearing on the answering of the research questions and the achievement of the research objectives.

6.12 CONCLUSION

A qualitative approach was used to understand the insight of the research participants on the use of Intelligence-Led Policing to combat cybercrime in South Africa. A phenomenological research design was used to understand the lived experiences of

police officers who are involved in the policing of cybercrime. The researcher analysed data from the participants responses who were detectives from the South African Police Service, members of the Directorate for Priority Crime Investigations and members of crime intelligence of the South African Police Service by means of the Tesch data analysis method.

CHAPTER SEVEN: PRESENTATION, DISCUSSION AND INTERPRETATION OF RESEARCH FINDINGS

7.1 INTRODUCTION

This chapter focuses on the presentation, discussion and interpretation of the research findings of the study that are derived from the literature review presented in Chapter One to Chapter Six as well as the one-on-one semi-structured interviews with research participants. The one-on-one semi-structured interviews conducted with research participants were used to explore the use of Intelligence-Led Policing to combat cybercrime in South Africa. A phenomenological research design is applied in this study to address research questions and to achieve the research objectives. The research participants involved in this study are detectives from the South African Police Service, members of the Directorate for Priority Crime Investigation and crime intelligence members from the South African Police Service. They are members who are directly involved in the investigation of cybercrime in the Limpopo, Gauteng, Free State, Mpumalanga and North- West Provinces. A data saturation method was used during the empirical data collection, in which the researcher interviewed participants until no new information emanated from the interviewed participants as the interviewees simply repeated what had already been mentioned.

The interviews were audio-recorded and field notes were also taken to enhance the validity and trustworthiness of the collected data. Tesch's data-analysis method was used to interpret and analyse the collected data in order to understand the meaning of data received from the research participants, as well as detecting similarities and differences. After the data analysis the researcher transcribed the audio-recorded interviews into text to understand the use of Intelligence-Led Policing to combat cybercrime in South Africa.

7.2 FINDINGS

The findings of the study are categorised into the major eleven themes of this study, namely - the role of Intelligence-Led Policing in the investigation of cybercrime, investigative skills required in the investigation of cybercrime, the use of Intelligence-Led Policing by the South African Police Service to combat cybercrime, challenges encountered in using Intelligence-Led Policing to combat cybercrime, addressing

challenges encountered in using Intelligence-Led Policing to combat cybercrime, challenges encountered in the investigation of cybercrime, the impact of the challenges encountered in the investigation of cybercrime, addressing the challenges encountered in the investigation of cybercrime, the strategy of the South African Police Service in the investigation of cybercrime, the strategy of the Directorate for Priority Crime Investigation in the investigation of cybercrime, and the value of using Intelligence-Led Policing in the investigation of cybercrime in South Africa.

The findings on research objectives and the research questions are incorporated in the relevant specific findings that are indicated below as follows:

- The findings on the use of Intelligence-Led Policing by the South African Police Service to combat cybercrime that is contained in section 7.2.3 indicate the achievement of the second research objective that is contained in section 1.4 of this study, namely - the establishment of the extent to which Intelligence-Led Policing is used to combat cybercrimes as well as the research question on how Intelligence-Led Policing is used to combat cybercrimes in South Africa.
- The findings on the challenges encountered in using Intelligence-Led Policing to combat cybercrime as reflected in section 7.2.4 also encompass the third research objective that is contained in section 1.4 of the study that deals with the determination of the challenges encountered by the police in the use of the Intelligence-Led Policing in combating cybercrimes in South Africa; as well as the supplementary research question that is contained in section 1.5 of this study, which deals with challenges encountered by the police in the use of Intelligence-Led Policing to combat cybercrime in South Africa.
- The findings on the value of using Intelligence-Led Policing in the investigation of cybercrime in South Africa that is contained in section 7.2.11. includes the second research objective that is contained in section 1.4 of the study that relates to the establishment of the value of Intelligence-Led Policing in combating cybercrimes in South Africa.

The findings, interpretation and analysis in this Chapter are done in the context of both the literature and empirical findings. Individualised presentation of the findings on each

category of the respondents is done by presenting each specific category of the participants as detectives, members of the Directorate for Priority Crime Investigation or crime intelligence members. Where there is no distinct difference in their responses a collective presentation, discussion and analysis is done.

7.2.1 The role of Intelligence-Led Policing in the investigation of cybercrime

Section 3.7 and 5.8 of the literature review indicates that Intelligence-Led Policing helps crime investigators to collect, analyse, interpret and disseminate cybercrime information that facilitates the understanding and response of the police to cybercrime threats. It enables investigators to collect a large quantity of data for examination and interpretation to understand cybercrime patterns, trends and series in order to target cybercriminals. The collected data helps the police to identify cybercrime hotspots, thus making it easy for them (investigators) to profile and link cybercriminals to committed crimes and predict their future plans.

Detectives: The interviewed detectives concurred with the literature findings that Intelligence-Led Policing enables the police to collect cybercrime information that could be used to detect cyber threats and identify cybercriminals for arrest and prosecution. One detective stated that *“Intelligence-Led Policing in the investigation of cybercrime helps in gathering information that can be used to detect cyber threats, identify and apprehend cybercriminals”*. Another detective member elaborated on this by stating that *“Intelligence-Led Policing helps in the collection of crucial data on cybercrime in order to identify the prevalence of cybercrime in certain settings, the nature of such crimes and the characteristics of the people who commit them”*.

The above clearly indicates that the use of Intelligence-Led Policing in the investigation of cybercrime enables the police to collect relevant information on this type of crime, its commission and the people involved. It renders a comprehensive picture to the police that assists them in identifying and prosecuting the perpetrators of this crime; and the information collected also benefits crime prevention efforts by indicating the characteristics of the people most targeted as well as the most common methods used by the offenders. This sentiment is also echoed by one detective who stated that *“without the use of Intelligence-Led Policing in the investigation of cybercrime it could*

be difficult for the police to successfully investigate this crime and understand its characteristics and dynamics for effective policing.”

The above findings support what is discussed in the literature by various authors such as Budhram (2016), Fick (2019) and Buckley (2014). Budhram (2016: 85) believes that Intelligence-Led Policing can be used as crime management philosophy that can cluster cybercrime activities into one funnel through proactive cybercrime investigation techniques, cyber forensic methodology, targeting of prolific cybercriminals and apprehending cybercriminals. According to Fick (2019: 31) cybercrime investigators use Intelligence-Led Policing as end product for gathering and analysing cybercrime threats, tracing cybercriminals, detecting cybercrime in cyberspace, investigating and preventing cybercrime activities. Buckley (2014: 46) asserts that Intelligence-Led Policing enables the police to identify cyber-attacks that are active online and analyse them to link them to attacks that might happen in future. Budhram (2016: 86) also supports this by stating that the use of overt and covert methods by Intelligence-Led Policing in managing cyberspace can target cybercrime offenders and set traps to detect and investigate cyber-attack incidents.

Members of the Directorate for Priority Crime Investigation: Interviewed members of the Directorate for Priority Crime Investigation agreed with the sentiments of the detectives but provided elaborated responses which could be attributed to the nature and level of their involvement in the investigation of cybercrime. They clearly indicated that Intelligence-Led Policing helps in the proper collection and contextual analysis of cybercrime data. It helps in detecting, identifying, tracing and investigating cyber threats in cyberspace. Most members were convinced that it helps investigators to make informed decisions in the gathering of raw data on social media and Global Positioning System (GPS) coordinates to form a picture of cybercrime events that may lead to successful cybercrime investigation. The sentiments are made clear by one member who stated that *“the role of Intelligence-Led Policing in the investigation of cybercrime is to make well informed decisions in cybercrime investigations and gathering of raw data on social media and GPS coordinates to form a picture of cybercrime events that lead for successful cybercrime investigation”*. This is supported by the response from another member who stated that *“Intelligence-Led Policing leads to the focussed gathering of cybercrime evidence from digital system or cyberspace*

to identify and trace cybercriminals. Thus, providing technological data gathering and analysis of cybercrime activities to generate intelligence report”.

Another similar view expressed by some members is that Intelligence-Led Policing enables the investigators to detect potential cybercrime attacks, to gather and trace information relating to that and in the process inform and support investigators in the identification as well as the tracing of cybercriminals and potential cybercriminals. This form of policing enables the police to have the ability to prevent cybercrime as well as to develop strategies and techniques that could enhance their capability in the investigation of committed cybercrimes. One of the members elucidated this by stating that *“the role of Intelligence-Led Policing in the investigation of cybercrime is to prevent cybercrime before it takes place, it also helps in preparing the strategies and techniques to investigate cybercrime when it happens”.*

Other participants stated that Intelligence-Led Policing supports cybercrime investigators in gathering digital evidence in cyberspace and provides effective digital forensic support such as the seizure, analysis, preservation and presentation of digital evidence in court, thereby emphasising that Intelligence-Led Policing employs technological advances to generate valuable intelligence through collaboration with relevant stakeholders such as some members of the public who have valuable observation and information on possible cybercrime activities. They may provide historical cybercrime datasets using data mining and machine learning techniques useful to detect, predict and prevent cybercrime. It is useful in preventing or mitigating cyber-attacks by studying the cyber threats data and to provide information on adversaries and helps investigators to identify cybercrime by utilizing information sharing and collaboration between law enforcement agencies and communities. It locates cybercrime threats to find potential victims and repeat offenders in the data-driven approach by analysing cybercrime data that might accompany it in specific communities. This is clearly captured by the following three verbatim statements of three members: *“According to my understanding, Intelligence-Led Policing supports cybercrime investigators in gathering digital evidence”;* *“the role of Intelligence-Led Policing is to use technological advances to generate valuable intelligence collaborating with community members who have valuable observation and information. It provides historical cybercrime datasets using data mining and machine*

learning techniques to discover the useful knowledge that could detect, predict and prevent cybercrime”; “Intelligence-Led Policing helps to prevent or mitigate cyber-attacks by studying the cyber threats data and provide information on adversaries. It helps investigators to identify cybercrime by utilizing information sharing and collaboration between law enforcement agencies and communities to locate cybercrime threats, find potential victims and repeat offenders on the data-driven approach by analysing cybercrime data that might accompany it in specific communities”.

Crime intelligence members: Some crime intelligence members of the South African Police Service indicated that the value of Intelligence-Led Policing lies in its ability to provide law enforcement agencies with the intelligence and analysis to stay ahead of the constantly evolving cybercrime landscape. The participants indicated that using Intelligence-Led Policing can develop more effective strategies for prevention and detection of cybercrime and it works more collaboratively with other organisations to achieve its goals. This is emphasised by the statements from two members who stated that *“Intelligence-Led Policing makes the police stay abreast of new and emerging threats in cybercrime landscape. It helps the police in collecting and analysing data on cybercrime trends and tactics to develop more proactive approach for cybercrime prevention and detection rather than simply reacting on the incidents as they occur”.* The other member stated that *“according to my opinion, the value of using Intelligence-Led Policing is to effectively combat cybercrime, mitigate, prevent, reduce and combat cybercrime activities”.*

7.2.2 Investigative skills required in the investigation of cybercrime

Section s1.3 and 2.7 of literature review indicate that cybercrime investigators need to have knowledge, understanding and skills related to information technology to understand the dynamics associated with the nature, risks and advances in the investigation techniques of cybercrime. These sections emphasise that continuous in-house training in cybercrime investigation is required to equip investigators to gather evidence, retrieve evidence in cyberspace, detect cyber threats and trace suspects of cybercrime. Cyber forensic and cyber intelligence experts need to be used to investigate cyber- related crimes due to their knowledge and skills of tracing and

retrieving digital evidence on the sophisticated technology and borderless information networks.

Detectives: In support of the above, some of the interviewed members stated that cybercrime investigators should have knowledge and skills in the use of technology, analytical skills, clear communication skills and understanding of cybercrime laws. Such investigators should attend courses on information technology as well as being properly trained in cybercrime laws and other computer crime laws. One of the members emphasised this by stating that *“the investigation of cybercrime requires investigators to have technological and analytical knowledge and skills as well as the understanding of cybercrime laws. Have competency in problem solving, critical thinking, curiosity, good knowledge on human behaviour and technology savviness”*.

Police working on cybercrime should understand the recovery of the files or documents in the hacked system and the preservation of digital evidence in compliance with legal requirements for it to be admissible in court. The above requirements were emphasised by one of the participants as *“computer and internet skills, understanding of the South Africa constitution, criminal law, criminal procedure, cybercrime laws, law of evidence, and the skills in the investigation of fraud and corruption”*. This view is supported by another investigator who stated that *“cybercrime investigators need to be highly equipped and well trained in technology so that cybercrime information can be gathered easily, to positively trace suspected cybercriminals, successfully retrieve evidence of cybercrime online and safe keep the collected evidence for court purposes”*.

In support of what had been said by their colleagues above, some members mentioned that cybercrime investigators should have skills in report writing, problem solving and information monitoring. This could assist them in interacting with other law enforcement agencies for the successful investigation and prosecution of cybercriminals due to the borderless nature of this crime. Coupled with this, they should be knowledgeable on cybercrime investigation, criminal investigation, financial crime investigation and computer crimes to be able to conduct focused investigations. This was accentuated by one of the members who stated that *“cybercrime investigators must have knowledge of cybercrime investigation, criminal investigation,*

financial crime investigation and computer crime. These skills can assist investigators to be more accurate when conducting their investigation and to know where to focus during investigation of crime". Another member echoed that *"cybercrime investigators must have experience in computer crimes, intelligence analysis and threats analysis to be able to conduct cybercrime search to know the modus operandi of cybercriminals"*.

From the above three paragraphs it is clear that participants were unanimous on specific investigative skills required to investigate cybercrime effectively. The nature and character of cybercrime warrants comprehensive and inclusive knowledge and skills for its successful investigation and prosecution. Computer skills and fraud investigation skills coupled with the identification, collection and preservation of digital evidence as well as the knowledge of criminal law, criminal procedure, law of evidence and relevant cyber legislation form the core of requisite knowledge. Considering that cyberspace is a dynamic and continuously changing environment, the indicated continuous training for cybercrime investigators is absolutely essential to keep abreast of developments in this field. According to Basdeo, Montesh and Lekubu (2014: 62), cybercrime investigators need to have knowledge, experience and related training to be able to gather cybercrime information, identify and trace suspects as well as being capable to investigate cybercrime incidents effectively.

Members of the Directorate for Priority Crime Investigation: Concurring with the essence of the required skills that is indicated by the detectives, some of the interviewed members of the Directorate for Priority Crime Investigation included the academic knowledge that is required also, stating that for cybercrime investigators to investigate cybercrime effectively they require qualifications such as information technology, computer science, information science and forensic investigations. They believed that this will help them to have knowledge and understanding of cybercrime actions, cyber-security, cybercrime research, computer security breaches and cloud computing, equipping them to identify cyber threats on the electronic devices, data breaches and hacked computers. Four of the members expressed these requisites in the following statements: *"the required skills for cybercrime investigators are computer skills, networking skills, cloud computing and cybercrime investigation"; "the knowledge and skills required for the effective investigation of cybercrime are*

computer skills, background and knowledge on cybercrime act, knowledge relating to cyber-security, knowledge of information technology and knowledge of cybercrime investigative skills”; “investigate skills required for one to effectively investigate cybercrime are knowledge of online investigative skills, open-source intelligence investigative skills, social media investigative skills, organised crime investigative skills and commercial crime investigative skills”; and “investigative skills that are required for one to effectively investigate cybercrime are information technology, information science and computer science expertise to be able to identify cyber threats on the cyberspace as well as the ability to monitor and investigate any cyber threats on electronic devices”.

7.2.3 The use of Intelligence-Led Policing by the South African Police Service to combat cybercrime

Members of crime intelligence indicated that the South African Police Service uses Intelligence-Led Policing products like Signal Intelligence, Open Source Intelligence and Human Intelligence to combat cybercrime activities. The role of Signal Intelligence is to monitor and identify incoming and outgoing data in electronic devices, Open Source Intelligence helps in the collection of large quantities of cybercrime data that can be used in threat alerts, while Human Intelligence is used as surveillance to detect, identify and locate emerging trends and threats on the electronic device to combat cybercrime (Veerasingam, 2017: NP). The South African Police Service uses Intelligence-Led Policing to target cybercrime offenders by using overt and covert intelligence methods for targeting crime in cyberspace, trapping cybercrime offenders through monitoring cybercrime hotspots and implementing cybercrime security measures to combat it (Budhram, 2016: 86). The South African Police Service also uses Intelligence-Led Policing products such as the Geographical Information System to identify cybercrime hotspots, responses to cybercrime, prevention of cybercrime and the understanding of cybercrime distribution to combat it (Santos, 2013: 95). These technologies help South African Police Service members to predict exact locations of cybercrime, detect crime activities, cybercrime hotspots and predict the places of cybercrime offenders (Ratcliffe, 2016: 151). Some of the crime intelligence members stated that *“the South African Police Service use Intelligence-Led Policing to collect intelligence information on cybercrime including the trends and patterns of cybercriminals. This information is used to identify potential threats and to develop*

proactive strategies to prevent and combat cybercrime” the other member stated that “according to my knowledge, Intelligence-Led Policing is used by the South African Police Service for conducting risk assessments to identify vulnerabilities in critical infrastructure and to assess the potential impact of cyber-attacks to combat cybercrime. This information is used to develop plans to prevent cyber-attacks and to respond quickly in the event of a cyber-attack”.

Other crime intelligence members indicated that the South African Police Service uses Intelligence-Led Policing for collecting intelligence information, conducting risk assessments, developing partnerships, using technology, providing training and capacity building to officers and investigators to improve their knowledge to have a better understanding on the importance of using Intelligence-Led Policing to combat cybercrime. The use of Intelligence-Led Policing provides a more proactive and effective response to cybercrime, thus protecting South Africans and critical infrastructure. Intelligence-Led Policing is a proactive cybercrime prevention strategy that involves the collection and analysis of intelligence information to guide police activities and operations. This was emphasised by one member of crime intelligence who stated that *“Intelligence-Led Policing is used by the South African Police Service through working together with other law enforcement agencies, government agencies and private sectors to share intelligence information and coordinate activities to combat cybercrime. The sharing of intelligence and collaboration allows for more effective targeting of cybercriminals and better use of resources to combat cybercrime”.* Another member of crime intelligence stated that *“In my understanding, Intelligence-Led Policing by the South African Police Service use advanced technology such as data analytics and artificial intelligence to collect, analyse and share intelligence information to combat cybercrime. This technology helps for faster and more accurate identification of potential threats and more effective targeting of cybercriminals”.* While the other member stated that *“according to my knowledge, Intelligence-Led Policing is used by the South African Police Service to provide training and build capacity for police officers and investigators to improve their understanding of cybercrime and to develop their skills in order to effectively investigate and prosecute these crimes”.*

The literature research also revealed that Intelligence-Led Policing is used by the South African Police Service to collect and analyse cybercrime information for operational, tactical and strategic decisions on combating cybercrime (Buckley: 2014: 32). It is used in reducing, preventing, disrupting and combating cybercrime activities through identifying cybercrime hotspots, cybercrime locations, cybercriminals and victims to make appropriate decisions (Ratcliffe, 2016: 65). It can also be used for gathering and collecting large quantities of cybercrime data as well as examining and interpreting cybercrime data to understand cybercrime threats, patterns, trends and series (Ronczkowski, 2012: 115). It indicates that it is also usable in intervening and disrupting cybercrime activities by using intelligence end products to make decisions. In support of these, some interviewed crime intelligence officers stated that *“Intelligence-Led Policing is used for the collection and analysis of data on cybercrime trends, tactics and actors. They use data to identify and prioritise high-risk targets to allocate their resources more effectively and to develop strategies for preventing and detecting cybercrime”*. While the other member stated that *“according to my opinion, Intelligence-Led Policing is used for the gathering and collection of credible information from reliable sources before the commission of cybercrime and the information that could be used to combat cybercrime where normal crime prevention approaches fail to prevent it”*.

Some crime intelligence members stated that Intelligence-Led Policing is used by the South African Police Service to gather, collect, analyse and disseminate cybercrime data to identify suspects, trace them, identify cybercrime locations and arrest suspects to combat cybercrime activities. This form of policing helps the police to detect, prevent, investigate and combat cybercrime. It is also used for developing cybercrime security measures that can be used to target high-risk cybercriminals, identifying cybercrime hotspots, identifying people associated with cybercrime incidents and their businesses for effectively combating it. These sentiments are articulated by some of the interviewed crime intelligence officers as *“in my opinion, Intelligence-Led Policing is used by the South African Police Service to combat cybercrime by detecting it, identifying suspects, identifying evidence related to cybercrime activities, tracing suspects and arresting them for prosecution”*; *“according to my understanding, Intelligence-Led Policing is used by the South African Police Service to identify cybercrime hotspots, locations of cybercrime, identifying people associated with*

cybercrime activities, gathering and collection of data related to cybercrime”; while the other one stated that *“Intelligence-Led Policing is used by the South African Police Service for collecting cybercrime information and conducting risk assessment to identify cybercrime threats in order to develop effective cybercrime prevention and combating strategies”*.

7.2.4 Challenges encountered in using Intelligence-Led Policing to combat cybercrime

The literature indicates some of the challenges encountered in using Intelligence-Led Policing to combat cybercrime as substantive ambiguity of the conceptual implementation (Cartex & Fox, 2018: 2). There is lack of evidence to show how Intelligence-Led Policing is used by the police to deal with cybercrime. Ezeji (2017: 167) states that the failure of the police to use Intelligence-Led Policing to combat cybercrime is because the police is labelling it as subterfuge - a clandestine and covert activity that is used by police to conduct illegal means in the name of intelligence. Lack of resources and training amongst the police to combat cybercrime is another challenge in the use of Intelligence-Led Policing (Cichoracki, 2020: 6). According to Zinn (2011: 11), lack of data on cybercrime, lack of research on Intelligence-Led Policing and the public scrutiny on research about the use Intelligence-Led Policing to combat cybercrime are some of the challenges encountered in the use of Intelligence-Led Policing to combat cybercrime. Some interviewed crime intelligence members voiced the above challenges in the use of Intelligence-Led Policing by stating that *“in my opinion, the police may struggle to keep up with the latest technological advancements and may lack the technical expertise needed to use Intelligence-Led Policing effectively to combat cybercrime”*; *“according to my understanding, the Intelligence-Led Policing could be resource-intensive and require significant investment in technology, training and personnel. The police may lack the resources needed to implement effective Intelligence-Led Policing strategy to combat cybercrime”*; and *“the police may encounter legal and ethical challenges related to data privacy and security which can limit the ability to collect and use data in an Intelligence-Led Policing strategy to combat cybercrime”*.

Other members of crime intelligence supported the above sentiments by stating that the challenges encountered in using Intelligence-Led Policing to combat cybercrime

are lack of skills, experience and training amongst police to effectively implementing Intelligence-Led Policing to combat cybercrime. The lack of resources and personnel are some of the challenges encountered in using Intelligence-Led Policing because without personnel and resources the implementation of Intelligence-Led Policing to combat cybercrime will be difficult. Some crime intelligence members explained that the advanced technologies that are used by cybercriminals to commit cybercrime make it difficult for the police to keep in pace with cybercrime. One member said that *“in my opinion, the police may encounter jurisdictional issues when trying to combat and prosecute cybercrime across international borders and this can make it difficult to effectively use Intelligence-Led Policing techniques in combating cybercrime”*. The sentiments of this member were supported by another member who stated that *“cybercrime tactics and technologies are constantly evolving, making it difficult for the police to keep pace with them and make it challenging to develop effective Intelligence-Led Policing strategy that are able to keep up with the latest threats”*.

7.2.5 Addressing challenges encountered in using Intelligence-Led Policing to combat cybercrime

Most crime intelligence members, supported by the literature, indicated that to overcome some of the challenges encountered in using Intelligence-Led Policing there is a need to change the police culture of relying on reactive policing, the need for good leadership in policing, and the proper understanding of using Intelligence-Lead Policing in detecting, reducing, preventing and combating cybercrime. Ratcliffe (2016: 192) emphasises that encountered challenges can be addressed through establishing national and international partnerships with law enforcement agencies around the world, together with communities, government agencies and the private sector, highlighting the need to use Intelligence-Led Policing in helping to combat cybercrime. He further states that some of these challenges can be addressed by a good top-town leadership style that provides leadership from uniform, traffic and detective resources as well as proving guidance to the police on how resources should be employed in using Intelligence-Led Policing to combat cybercrime (Ratcliffe, 2016: 65). Some of the challenges can be addressed by employing many experienced personnel, training them and providing leadership at operational level to help in implementing the use of Intelligence-Led Policing to combat cybercrime (Ezeji, 2017: 357). Some of the crime intelligence officers articulated this by stating that *“in my opinion, the encountered*

challenges can be addressed if the South African Police Service can train and hire personnel with specialised technical expertise in cyber-security, digital forensic and other relevant areas on information technology. This can help to ensure that the South African Police Service personnel have knowledge and skills needed to effectively combat cybercrime". The other one stated that *"encountered challenges can be addressed if the South African Police Service can partner with other organisations such as the private sector and academic institutions to access resources and expertise that they may not have in-house. This can help the South African Police Service to address resource limitations and technical expertise challenges".*

A number of the interviewed crime intelligence members indicated that some of the encountered challenges can be addressed through a multi-faceted approach that involves investing in training, technical expertise, leveraging partnerships, enhancing data privacy and security, coordinating across international borders and keeping up-to-date with latest cybercrime threats. Intelligence-Led Policing could be an effective strategy to detect, prevent, investigate and combat cybercrime activities. These are clearly articulated in the following statements from some crime intelligence members - *"in my understanding, the encountered challenges can be addressed by developing protocols for handling and storing sensitive data and ensuring that they are in compliance with relevant data privacy laws and regulations. They can work with organisations such as Computer Emergency Response Teams, Financial Intelligence Centre and South African Banking Risk Information Centre to develop best practices for securing data and system to combat cybercrime"; "the encountered challenges can be addressed by establishing international partnerships to develop coordinated strategies for investigating and prosecuting cybercrime across borders. This can involve developing protocols for sharing information and evidence of cybercrime as well as building relationship with law enforcement agencies in other countries".* While the other one stated that *"the encountered challenges can be addressed by investing in ongoing police training and professional development to ensure that they are up to date with the latest cybercrime trends and tactics. They can also leverage intelligence sharing platforms and other resources to stay abreast of emerging threats and adjusting their Intelligence-Led Policing strategies accordingly".*

7.2.6 The challenges encountered in the investigation of cybercrime

According to section 1.2, 2.7, 2.8 and 5.7 of the literature research, some of the challenges in the investigation of cybercrime are that it could be perpetrated by a person anywhere in the world who is positioned far away from the victim. Kopelev (2000: 60) states that cybercrime data might be situated in different countries and not be in the country where the cybercrime has occurred and this makes the investigation process difficult. It requires effective cooperation amongst law enforcement agencies around the world to have mutual agreements on extradition between countries. This in itself tends to involve various states with different legislation, thereby compounding the investigative process. This sentiment was clearly articulated by one member of the Directorate for Priority Crime Investigation who stated that *“the challenges encountered in the investigation of cybercrime are associated with national legal framework on cybercrime, obstacles of international cooperation with other countries during the investigation, and challenges around public and private partnership during the investigation”*.

Secondly, the literature and responses from some detectives and members of the Directorate for Priority Crime Investigation indicate the lack of resources coupled with the lack of sufficient and current training that could enable cybercrime investigators to detect criminal acts, identify cybercriminals, identify digital evidence required, collect such digital evidence and preserve it for successful prosecution as a major challenge. As one member of the Directorate for Priority Crime Investigation explained *“the challenges encountered in the investigation of cybercrime is improper handling of electronic evidence and lack of experience amongst investigators in the gathering of digital evidence which fails to comply with our admissibility rules that makes digital evidence being rejected by courts”*. These are the sentiments that are also clear from another detective who stated that *“In my experience as investigator, the lack of resources, knowledge and experience related to cybercrime is the biggest challenge encountered during cybercrime investigation. The lack of proper and adequate training on cybercrime investigation and lack of resources needed to investigate cybercrime such as licence and cyber forensic tools is a challenge facing cybercrime investigator”*. The licence matter was also articulated by another detective who complained that once it expires it takes a long period to be renewed. The participant’s direct words are *“in my viewpoint, the challenge encountered in the investigation of cybercrime is that*

when the licence that empowers one to investigate cybercrime expires, it takes long for it to be renewed, and this creates a back-log on cybercrime cases that are being investigated as it takes a long-time to finalise these investigations". Another member of the Directorate for Priority Crime Investigation contrasted the available resources and the high number of cybercrime incidents by stating that *"the challenges encountered by investigators in the investigation of cybercrime is a jurisdictional boundary that prevent cybercrime suspect from being prosecuted, too many cybercrime incidents and too little resources, lack of technical expertise and capacity to deal with cybercrime"*.

The licence to investigate cybercrime is issued to cybercrime investigators, enforcement agencies and private individuals who perform digital or electronic forensic investigations. The purpose of the digital forensic licence is to provide functionality that enables forensic extraction of data from electronic devices for analysis and evidential proof (Arnes, 2018: NP). The licence is issued by forensic vendors such as Encase, XRY and Data Pilot. Encase helps cybercrime investigators to conduct in-depth analyses to recover evidence like documents, pictures, internet history and windows registry information (Casey, 2011: 48). XRY helps cybercrime investigators to analyse and recover information from electronic devices and it has hardware devices that connect phones to computers and software to extract data (Jones & Winster, 2017: 8). On the other hand, Data Pilot helps cybercrime investigators to collect digital evidence to review images, videos, messages and application data from mobile phones or any electronic devices (Casey, 2011: 48). The digital forensic licence can be valid for 3-5 years and it depends on how much the procurer is willing to pay for the licence which may cost R75 000 to R100 000 per year (Arnes, 2018: NP). Without these licences investigators cannot get access to all the functionalities of forensic tools, they have limited access to the data or evidence (Casey, 2011: 48). The South African Police Service and the Directorate for Priority Crime Investigation rent these licences from the forensic vendors (companies). They (South African Police Service and the Directorate for Priority Crime Investigation) are responsible for the payment of the annual fees and the renewal of the respective licences for their investigators.

Lack of training and expertise was also indicated by one of the members of the Directorate for Priority Crime Investigation as *"according to my opinion, the challenges*

encountered in the investigation of cybercrime is lack of experience, training and manpower". In support on this, the response from another member of the Directorate for Priority Crime Investigation was *"the challenges encountered in the investigation of cybercrime is a lack of resources, lack of knowledge, training and experience related to cybercrime"*. From the interviews with members of the Directorate for Priority Crime Investigations it became clear that lack of specific tools that should enable them to perform their duties is also a problem as it could be detected from these statements *"the challenges encountered in the investigation of cybercrime is inadequate digital forensic tools to gather electronic evidence"*; and *"in my opinion, the challenges encountered in the investigation of cybercrime is the loss of cybercrime data, encryption of data and the lack of proper cybercrime collection evidence tools for the search and seizure of cybercrime evidence"*.

Thirdly, the sophistication of cybercrime offenders to hide their identities and use other people's identities during the commission of cybercrime, makes it difficult for cyber investigators to identify and investigate them. Fourthly, the expensive nature of cybercrime due to its inclination to warrant cybercrime investigators to travel to other countries, establish cooperation and conduct joint investigations with other law enforcement agencies exacerbate the problem. The above literature findings could be summarised in part by the statement from one of the detectives who opined that *"there are too many cyber-security incidents, too little cybercrime investigators, lack of resources, lack technical expertise and lack of capacity to keep up with cybercrime incidents"*.

Some of the interviewed detectives indicated factors such as lack of resources, lack of training, shortage of skilled and experienced cybercrime investigators as some of the factors that inhibit effective and efficient investigation of cybercrime. One of the participants emphasised this by stating that *"the challenge encountered in the investigation of cybercrime is the lack of resources (manpower, equipment and budget) to be utilised in cybercrime investigation"*. The explanation of these factors covers the training and the financial cost involved in the investigation of this crime that is explained by the literature in the preceding paragraph. There is a lack of harmonised legislation required to investigate this crime effectively which is the direct result of the

borderless nature of this crime as indicated on the first challenge that is reflected in the preceding paragraph.

Added to these multitudes of challenges, some of the detectives indicated the lack of international cooperation and public-private partnership that could present a united and coordinated front in the fight against cybercrime. They indicated that in some instances it is hard to find tangible digital evidence because of the high volatility of digital evidence and ways of hiding it. This is compounded by the lack of expertise in terms of knowing where to look and what to look for because the quality of digital evidence found and its preservation have a bearing on successful investigation and successful prosecution. In some cases, victims are unwilling to testify because they fear they would lose their clients and they want to protect the reputation of their companies. The words of one of the detectives echoed this: *“the challenge encountered in the investigation of cybercrime is the unwillingness of victims to testify for fear of being stigmatised or losing clientele. For example, Banks, Automobile Industry and Insurance Companies are often not willing to pursue cyber-attack cases for fear of losing clientele and the negative image that their companies might have”*.

The above sentiments are supported by another member of the Directorate for Priority Crime Investigation who stated that *“In my understanding, the challenges of cybercrime investigation is a lack of cooperation from service providers who normally delays the investigation process, improper handling of electronic evidence and lack of experience in the gathering of evidence, refusal of victims to testify in court, fear of stigmatisation, long-term period of gathering evidence and inadequate digital cyber forensic tools for gathering and packaging electronic evidence”*. Another member of the Directorate for Priority Crime Investigation also supported this by stating that *“According to my opinion, the lack of resources, insufficient cybercrime information from complainants or witnesses, refusal of witnesses to testify in court during prosecution of cybercriminals and limited budget are the challenges encountered by cybercrime investigators”*.

7.2.7 The impact of the challenges encountered in the investigation of cybercrime

The findings of the literature in section 2.7, 2.8, 3.6, 5.6 and 5.7 point out that the trans-border nature of cybercrime makes it difficult to trace, identify and apprehend offenders. It makes it very difficult for cybercrime investigators to detect cybercrime threats, retrieve digital evidence and trace suspects. Most detectives and members of the Directorate for Priority Crime Investigation indicated that lack of sufficient training for cybercrime investigators delays the investigations because investigators take long to resolve cases which could have been done much quicker if they were dealt with by trained and skilled people. Victims of such crimes do not see justice being done and lose trust in the criminal justice system, thus becoming reluctant to report these cases and being involved in the prosecution of suspected offenders by testifying in future. One member of the Directorate for Priority Crime Investigation put it as follows: *“cases of cybercrime investigations are taking too long to be finalised thus impacting on successful investigation and speedy trial. Then victims tend not get the justice they deserve and ultimately end-up losing hope for police and their investigation processes”*. Another detective echoed this by stating that *“lack of skilled cybercrime investigators leads to poor investigations that results in unsuccessful prosecution”*. The sentiments of this detective are supported by one member of the Directorate for Priority Crime Investigation who stated that *“some incidents of cybercrime remain undetected and unsolved because of the lack of experience and training of cybercrime investigators”*. The impact from the lack of resources perspective is indicated by some detectives as leading to unsuccessful investigations and the continuous postponement of cases that are ultimately struck off the roll due to lack of evidence. Another detective stated that *“lack of resources and cybercrime investigators leads to unsuccessful investigation because the deadline for data collection and analysis lapse”*.

7.2.8 Addressing the challenges encountered in the investigation of cybercrime

The findings of the literature in section 1.2, 2.4, 2.7 and 2.9, outline that the challenges can be addressed by empowering cybercrime investigators through training to obtain knowledge and skills on how to detect, prevent and investigate cybercrime. They will be empowered to identify, collect and preserve critical digital evidence according to the prescripts of the law to ensure its admissibility in court. These sentiments are echoed by most detectives and members of the Directorate for Priority Crime

Investigation as reflected in the direct quotes of some of them such as *“the challenges can be addressed by continuous training and workshopping of cybercrime investigators on cybercrime incidents. As well as providing cybercrime units with cybercrime investigation equipment’s”; “the challenges can be addressed through allocation of resources to the cybercrime investigators and empowering them with the knowledge and skills through workshops and training courses related to cybercrime”;* and *“providing proper training, proper equipment’s and relevant information to the investigators can help to address the challenges”*. In addition, one member of the Directorate for Priority Crime Investigation included the need to educate the community about cybercrime by stating that *“the challenges can be addressed by educating the communities about cybercrime and providing cybercrime investigators with training of cybercrime investigation”*. The involvement of other stakeholders is supported by another member of the Directorate for Priority Crime Investigation who explained that *“some of the challenges can be addressed through building international cooperation for cybercrime investigations, improving their technical capabilities and the sharing of information about cybercrime activities with other cybercrime investigators”*.

Some of the detectives and members of the Directorate for Priority Crime Investigation pinpointed the need to appoint the right people with appropriate qualifications in the investigation of cybercrime by asserting that *“to address the challenges there is a need to employ people with right qualifications, knowledge and skills to be able to investigate cybercrime”*. Another participant reiterated that *“to address the challenges require the police department should appoint the investigators who have appropriate qualifications, skills, experience and knowledge to deal with cybercrime investigations”*. He indicated that the challenges can be addressed by employing cybercrime investigators with the correct credentials such as skills, knowledge, experience and qualifications. Such members should then be supported with continuous training and sophisticated equipment to meet the challenging and dynamic nature of cybercrime. One of the Directorate for Priority Crime Investigation emphasised *“according to my understanding, some of the challenges can be addressed by providing investigators with advance software that can be use in different electronic devices to by-pass the passwords in detecting, identifying and tracing cybercrime threats on electronic devices”*.

7.2.9 The strategy of the South African Police Service in the investigation of cybercrime

The Cybercrime Act 19 of 2020 is used by the South African Police Service to deal with cybercrime investigation and empowers the police to development an anti-cybercrime strategy to provide training and the investigation capacity to ensure that cybercrime activities are detected, prevented and investigated effectively (Chitimira & Ncube, 2021: 20). Most interviewed detectives are not sure on what the cybercrime investigation strategy is and whether the South African Police Service does have a strategy to deal with cybercrime. They confuse the strategy with the available legislation, as detected from the following statements, namely, *“the South African Police Service has a focused cybercrime strategy that deal with cybercrime investigation which is a Cybercrime and Security Bill of 2015, it guide cybercrime investigators in terms of procedures on how to search, access, seize and investigate cybercrime incidents on the internet”*; *“South African Police Service does indeed have a cybercrime strategy such as the Electronic Communications and Transactions Act 25 of 2002, the purpose of this strategy is to ensure that police enforce the law to prevent, investigate and arrest any person involved in cybercrime activities”*; *“cybercrime strategy is implemented within the South African Police Service through the South African Police Service Act 68 of 1995 that empowers the police to combat, prevent, investigate, search and seize any goods for any crime including cybercrime”*; and *“South African Police Service has cybercrime strategy which is Cybercrime Act 19 of 2020, the importance of this strategy is to empower investigators to enter any premise, search and seize any evidence believe to be used for cybercrime for investigation in accordance with the law”*.

The few detectives who seem to understand the difference between the legislation and strategy indicated that the South African Police Service does not have a strategy to deal with cybercrime. Their different opinions are *“the South African Police Service does not have a strategy to deal with cybercrime because most of the investigators do not know what is cybercrime, do not know the procedure they need to follow to investigate cybercrime successfully and do not know what equipment must be used to collect and analyse digital evidence”*; while another one stated that *“the South African Police Service do not have a focused strategy to deal with cybercrime currently, they*

are still busy establishing cybercrime units and the investigators are still in the learning phase”.

7.2.10 The strategy of the Directorate for Priority Crime Investigation in the investigation of cybercrime

The effective and focused approach that is used by the Directorate for Priority Crime Investigation members to deal with cybercrime investigation helps them to share information related to cybercrime activities with national and international law enforcement agencies for the cooperation and mutual assistance in the investigation of cybercrime (Phahlamohlaka & Hefer's, 2019: 5). This helps investigators of the Directorate for Priority Crime Investigation to build mutual agreements between countries and establish detection, prevention, mitigation and investigation of cybercrime measures. This approach gives them the responsibility to enter premises, search, seize and investigate any information related to cybercrime activities (Bogopa, 2020: 7). The focused approach enables the investigators of the Directorate for Priority Crime Investigation to investigate incidents of cybercrime within the country and provide the investigators with the responsibility to detect, prevent and investigate cybercrime 24/7 (Ntsaluba, 2017: 74).

All the members of the Directorate for Priority Crime Investigation, just like the detectives, conflate the strategy and legislation indicating that the cybercrime strategy guides members of the Directorate for Priority Crime Investigation investigators on how to detect, prevent and investigate cybercrime successfully. In addition, it guides investigators of this Directorate on how to enter premises, search and seize any evidence suspected to be used in cybercrime activities. The strategy of the Directorate for Priority Crime Investigation enables it to establish international cooperation and mutual assistance with other law enforcement agencies in different countries for joint cybercrime investigations. Furthermore, the strategy helps the Directorate for Priority Crime Investigation investigators to locate, trace, identify and arrest offenders of cybercrime activities, whether cybercrime occurs within South Africa and outside the country. Their answers conflate the strategy with legislation as it could be seen from the following statements: *“the Directorate for Priority Crime Investigation have a focused strategy that deals with cybercrime investigation, it use Electronic Communications and Transactions Act 25 of 2002 to enter any place with warrant or*

without warrant, search any articles or information related to cybercrime incidents and seize any articles or information as evidence for cybercrime investigations”; “the Directorate for Priority Crime Investigation have focused strategy to deal with cybercrime investigation which is a Cybercrime and Cyber-Security Bill of 2015, the purpose of the strategy is to empower the Directorate for Priority Crime Investigation members to enter any premises, search and seize any information alleged to be used in cybercrime activities as evidence for cybercrime investigations”; “the Directorate for Priority Crime Investigation have cybercrime investigative strategy, it use Cybercrime Act 19 of 2020 and these strategy help investigators to enter any premises to search and seize any evidence believed to be used in cybercrime activities and collect evidence that can be used in cybercrime investigation”; and “the Directorate for Priority Crime Investigation have focused strategy to deal with cybercrime which is Cybercrime Act 19 of 2020, it give the Directorate for Priority Crime Investigation members the responsibility to detect, prevent and investigate cybercrime within South Africa and establish international cooperation with law enforcement agencies of other countries to combat and investigate cybercrime”.

7.2.10.1 Cybercrime Strategy for the South African Police Service and the Directorate for Priority Crime Investigation

The South African Police Service and the Directorate for Priority Crime Investigation do not have a cybercrime strategy. The intensive literature search revealed that no police department in Africa has a dedicated cybercrime strategy. The Scotland Police, Federal Bureau of Investigation, and Victoria Police are some of the police agencies that have dedicated cybercrime strategies in Europe and the United States of America.

- **Scotland Police** - The Scotland police established a cybercrime strategy that guides the police not only to investigate incidents of cybercrime but also to gather, collect, analyse, assess and disseminate cybercrime intelligence that allows the police to establish worldwide cybercrime strategic intelligence sharing partnerships (Scotland Police Authority, 2020: 38). The intelligence products can help the police to prevent and disrupt cybercrime activities through the support and enhanced police approach for detection and pursuing of cybercrime offenders. This strategy guides the police to identify the behaviours online that can cause harm to electronic devices and to ensure that the police target cybercrime offenders appropriately. The police use digital tool

capabilities to identify and get involved where people are at risk of cyber threats or people are offending (Scotland Police Authority, 2020:39).

Digital tools allow the police to identify threats and respond appropriately. The use of digital tools helps to disrupt criminal activities, to identify cyber threats and to scale online threats to organised cybercrime syndicates that are seeking to exploit electronic devices (Scotland Police Authority, 2020: 39). Therefore, an effective strategy guides police management to train more police to use computers or electronic devices together with the forensic tools at their disposal to disrupt any form of cybercrime and to create a hostile environment that will deter cybercrime. Police digital and technological capability will help them to build and up-skill the police force with the skills and knowledge to ensure that police will be empowered to provide efficient and effective cybercrime investigation. The digital and technological capabilities help the police to be agile, efficient, resilient and secure in the use of information technology against cybercrime (Scotland Police Authority, 2020:40-41). Such strategy guides the police with the identification, recovery, investigation, validation and presentation of digital evidence found in the electronic devices or digital storage media devices for court or criminal proceedings.

- **Federal Bureau of Investigation** - The Federal Bureau of Investigation cybercrime strategy's focus is not only to investigate and combat cybercrime but also to confront the challenges facing cyberspace (Federal Bureau of Investigation, 2020). The Federal Bureau of Investigation strategy focuses on investigating crime, gathering intelligence relating to cybercrime and collecting intelligence for preventing and combating cybercrime activities. The purpose of this strategy is to ensure that American people have safety, security and confidence to be digitally connected within the country. The safety measures stipulate that cybercriminals and national state actors who compromise American digital space will be held accountable and targeted through indictments, red notices to sanctions, diplomatic pressure and cyber operations. The strategy provides the security through alerting American citizens about the system and network vulnerabilities that are derived from intelligence that is provided by the Federal Bureau of Investigation and its

partners (Federal Bureau of Investigation, 2020). The bureau notifies the target (individuals, companies and government departments) about cyber threats before the target may experience cybercrime and provides them with necessary information about the cybercrime to prepare and defend themselves against such cybercrime (Federal Bureau of Investigation, 2020). The Federal Bureau of Investigation provides confidence to the people of America by combating cybercrime threats with fierce urgency and to ensure that victims receive the necessary attention they deserve. The strategy empowers the bureau members to work 24/7 to ensure that they work with businesses, companies and government departments to break down the walls of cybercrime threats as a united front (Federal Bureau of Investigation, 2020).

- **Victoria Police** - The Victoria Police cybercrime strategy focuses on prevention, disruption, investigation, supporting victims and reporting (Victoria Police, 2022: 13). The Victoria police work together with communities to raise awareness and education about the risks of cybercrime so that communities can have knowledge to feel empowered to protect themselves as a cybercrime prevention approach. The Victoria Police strategy supports the strength of relationships between police, government and non-government organisations for preventing cybercrime, combating cybercrime and cyber security awareness campaigns (Victoria Police, 2022: 14). The police work together with their partners to reduce the communities' vulnerability about the cybercrime threats and to strengthen resilience to cybercrime across communities of Victoria. Disruption of cybercrime activities is one of the effective strategies of the police to prevent victimisation and to reduce the harm of cybercrime within communities (Victoria Police, 2022: 14). The police disrupt cybercrime activities by denying the offenders opportunities to relocate or to rebuild accounts to take over or disable digital forums. The strategy provides the police with the responsibility to support victims with a victim-centred policing service. The Victoria police have members that have the appropriate skills and knowledge to provide the best quality service and consistent cybercrime victim support. It trained frontline members to have knowledge, skills and protocols to assist victims who report cybercrime with the possible best service (Victoria Police, 2022: 18-23).

7.2.11 The value of using Intelligence-Led Policing in the investigation of cybercrime in South Africa

Intelligence-Led Policing is valuable in detecting, tracing, identifying, preventing and investigating cybercrime activities that are active in cyberspace (Buckley, 2014: 46). It helps cybercrime investigators to identify cyber threats through the use of intelligence assessment (Myeza, 2019: 116). According to Hartfied and Kwewen, (2008: 9), it can further be used to identify, trace, collect and target cybercriminals through interpreting, verifying and disseminating cybercrime information to understand cybercrime hotspots, the place of cyber incidents and the people associated with cybercrime activities. The literature discussed in section 4.2.4 has revealed that Intelligence-Led Policing technologies like intrusion cyber system detection, cyber threat intelligence and cyber surveillance are used by cybercrime investigators to detect, trace and target the in-coming data and out-going data online 24/7 to prevent and investigate of cybercrime. Widdsup et al. (2018: 600) further state that Intelligence-Led Policing is used for cyber risk assessment testing, identification of cyber threats in cyberspace, tracing of cybercriminals, content identification for detection and investigation of cybercrime.

Interviewed detectives and members of the Directorate for Priority Crime Investigation also supported the literature by indicating that Intelligence-Led Policing assists the police to gather cybercrime data to comprehend cybercrime hotspots, the location of cybercrime incidents and people associated with cybercrime activities. This is evident in the following statements *“Intelligence-Led Policing helps investigators to understand cybercrime hotspots, identify cybercrime location in details and people associated with cybercrime activities”*; and *“according to my understanding, Intelligence-Led Policing helps cybercrime investigators to detect, identify, trace, link and investigate cybercrime”*. They further stated that this may lead to the interpretation, verification, analysis and dissemination of cybercrime data to interrupt, prevent and investigate cybercrime. Cybercrime investigators should be assisted to identify cybercrime threats, cybercrime offenders, as well as to detect evidence in digital space to arrest cybercriminals and prosecute them to enhance future deterrence. These aspects are emphasised by one of the detectives who stated that *“the role of Intelligence-Led Policing in the investigation of cybercrime is the collection of larger quantity of*

cybercrime data for understanding cybercrime tactics during the commission of cybercrime, detecting cyber threats, tracing cybercrime offenders, interrupting their businesses, investigating cybercrime activities and prosecuting cybercrime offenders". The statement is supported by some members of the Directorate for Priority Crime Investigation who stated that *"the value of Intelligence-Led Policing in the investigation of cybercrime is gathering, collection, analysis, interpretation and dissemination of cybercrime data that can be used in cybercrime investigations"*; *"the value of Intelligence-Led Policing in the investigation of cybercrime helps investigators to understand cybercrime patterns, the trend and the linkage of cybercrime to assist them to investigate cybercrime"*.

7.3 CONCLUSION

Cybercrime is one of transactional crimes that is growing fast all over the world with huge investments in return and it has the advantage of low risk of detection. The lack of skills, experience and training amongst the police has a negative effect on the use of Intelligence-Led Policing to combat cybercrime. The literature review and interviews concurred that some of the challenges encountered in using Intelligence-Led Policing to combat cybercrime are the lack of personnel, limitation of resources, lack of training amongst police officials and lack of leadership amongst police management in the implementation of this model to combat cybercrime. The lack of partnership with the private sector and other law enforcement agencies is another contributing factor that has a negative effect on the use of Intelligence-Led Policing to combat cybercrime.

Most interviewed members do not have a clear understanding of the difference between strategy and policy, and they regard various policies and legislation that enable the South African Police Service and the Directorate for Priority Crime Investigation to deal with cybercrime as strategies. They do not know that a strategy is a unique plan designed to achieve the aim and the objective of the organisation. In a nutshell a strategy is a comprehensive plan, made to accomplish organisational goals, which in this case will be the effective and efficient policing on cybercrime. A policy, on the other hand is a set of rules made by the organisation for rational decision making that guides the organisation's current and future decisions. Conversely, a law (legislation) is the system of rules and regulations that are formulated and enforced by the administrative authority of a country to regulate human behaviour for the common

good; imposing penalties and punishments to the people who violate the prevailing laws. The lack of understanding of these three factors caused most participants to conflate them as if they are referring to one and the same thing.

With regards to the research questions and the research objectives the findings reveal that although the value of Intelligence-Led Policing cannot be underestimated, its use by the police to combat cybercrime is not clearly understood by most participants. The fear and suspicion regarding the extensive gathering of intelligence also raises some concerns on the possible misuse of such intelligence by the police. This is further compounded by the lack of resources and the unwillingness of some people to testify in fear of damaging the reputation of their organisations.

CHAPTER EIGHT: RECOMMENDATIONS AND CONCLUSION

8.1. INTRODUCTION

The challenges of cybercrime are constantly increasing with various cyber-attacks and different modus operandi adopted by cybercriminals daily. These offenders use their advanced technical abilities to access and carry out cybercrime attacks by means of the dark web and online black markets. The law enforcement agencies around the globe are confronted with various challenges when policing cybercrime, as is not an easy task to prevent and investigate because of its borderless nature. For the police to be able to detect, analyse and understand the threats of cybercrime they have to be innovative because traditional police methods and processes of dealing with traditional crimes are not necessarily successful when dealing with cybercrime. The use of Intelligence-Led Policing could lead to the effectiveness of their operations in preventing, combating and investigating cybercrime in an attempt to deal with rampant cybercrime incidents and threats.

The proper use of Intelligence-Led Policing can help police agencies around the globe in preventing, disrupting, investigating and reducing cybercrime activities and targeting offenders in cyberspace to enhance citizens' safety. It will enable the police to do network analysis and create personal profiling, maps and connections to be able to predict future cybercrime activities. The principle of crime control of Intelligence-Led Policing enables it to place cyber threats and risks into a holistic perspective to understand the impact of cybercrime on communities and enables the police to understand the impact of a wide variety of cybercrime problems and to realise the need to combat cybercrime across the globe. It should focus on cybercrime hotspots, prolific offenders and organised criminal groups to prevent and disrupt their future plans on cybercrime activities.

8.2. RECOMMENDATIONS

The recommendations in this chapter emanate from the identified shortcomings, gaps or challenges in the effective use of Intelligence-Led Policing in dealing with cybercrime. These recommendations are aimed at addressing the shortcomings of the current approaches and to enhance the effective and efficient prevention of cybercrime. They attempt to indicate what could be the best practices and methods

for the understanding of the use of Intelligence-Led Policing in combating cybercrime from a policing perspective.

The South African Police Service needs to address the conceptualisation and the implementation of Intelligence-Led Policing to combat cybercrime as well as various factors such as the misconceptions on Intelligence-Led Policing by law enforcement agencies; the importance of training to the police officers who deal with this crime and the critical resources that they need for the success of their operations in this regard; the challenges of expiring investigation licences that hinders investigators to access functionalities of forensic tools during the investigation; how to overcome the hidden identities which is a measure challenge on crime activities committed in cyberspace; how to address the fear of some cybercrime victims who are unwilling to testify based on the need to protect the reputation of their respective companies; and the impact of the lack of clear understanding of what cybercrime strategy is by most police officers as well as the effect of the absence of such strategy from both the South African Police Service and Directorate for Priority Crime Investigation.

8.2.1 Conceptual Implementation of the Intelligence-Led Policing

Based on the value of Intelligence-Led Policing as reflected in section 7.2.1, it is clear that there is no solid understanding on how the collected intelligence is used and to what extent it benefits crime prevention, crime combating and crime investigation activities. This is clearly indicated as the substantive ambiguity of the conceptual implementation of the Intelligence-Led Policing in section 7.2.4, as well as the indication that there is lack of evidence to show how Intelligence-Led Policing is used by the police to deal with cybercrime.

Based on this, the study recommends that the South African Police Service and the Directorate for Priority Crime Investigation develops a policy framework, guidelines and directives for police officials and members of the Directorate for Priority Crime Investigation to clearly understand the conceptualisation, implementation and the use of Intelligence-Led Policing in the prevention, combating and investigation of cybercrime. Secondly, to clearly understand the value of the comprehensive implementation and utilisation of Intelligence-Led Policing in the fight against cybercrime. There is also a need to clarify the substantive ambiguity that currently

exists within some members of the South African Police Service and Directorate for Priority Crime Investigation on Intelligence-Led Policing. Such clarity will highlight the significance of proper collection, dissemination and utilisation of collected intelligence in the fight against cybercrime.

The conceptual understanding of Intelligence-Led Policing and the clarification of the substantive ambiguity could go a long way in making police officers to understand the role of Intelligence-Led Policing in the identification of crime in the cyberspace for the rapid response and informed decision making on policing practices and strategies that could cope with the changing nature of this dynamic crime.

The development of the effective and efficient policy framework, guidelines and directives as well as their effective utilisation will be grounded on the following:

- Intensive research that will lead to the development of practical, effective and efficient policy framework, guidelines and directives;
- Intensive training/workshops on the developed policy framework, guidelines and directives so that members of the South African Police Service and the Directorate for Priority Crime Investigation clearly understand the policy framework, guidelines and directives, as well as their implementation and implication of such implementation. The training and workshops can help them to collect relevant evidence that is properly informed by the collected intelligence to prevent, combat and investigate cybercrime;
- Proper implementation coupled with the strategic utilisation of the allocated resources to ensure successful operations as well as the continuous monitoring of such operations to ensure that they achieve the desired results. That might also need constant modification of the implementation plans to adapt to the changing circumstances to ensure that the plans are fit for purpose.

8.2.2 Misconception on Intelligence-Led Policing

The failure of the police to use Intelligence-Led Policing to combat cybercrime is attributed to the misconception by some police officials that Intelligence-Led Policing is a subterfuge - a clandestine and covert activity that is used by police to conduct illegal means in the name of intelligence – as indicated in section 7.2.4. The misconception by some police officials regarding the use of Intelligence-Led Policing could be based either on their lack of knowledge on the concept of Intelligence-Led Policing or their experience in the misuse of intelligence by some police officials for their own nefarious actions.

The misconception that emanates from the lack of knowledge should be addressed by the police agencies themselves through workshops on the use and value of Intelligence-Led Policing in combating cybercrime. The police could also research and learn from other countries that adopted and successfully use Intelligence-Led Policing on how they addressed such mistrust of Intelligence-Led Policing by some members of their police agencies. The mistrust that is informed by the misuse of intelligence by some police officers could be dealt with by encouraging those police officials to report such incidents to the Inspector-General of Intelligence.

The Inspector-General of Intelligence has functional responsibility of monitoring and reviewing the intelligence and counter-intelligence activities of the State Security Agency, Defence Intelligence Division of the South African National Defence Force and Crime Intelligence Division of the South African Police Service. According to Section 7(7) of the Intelligence Services Oversight Act 40 of 1994 this includes monitoring compliance by any of these institutions with the constitution, applicable laws and relevant policies on intelligence and counterintelligence; review of intelligence and counter-intelligence activities by these institutions; the reception and investigation of complaints from members of the public and members of these institutions.

8.2.3 Lack of Resources, Training and Fear

The lack of resources and training amongst the police to combat cybercrime is another challenge in the employment of Intelligence-Led Policing. The challenge is compounded by the lack of research on Intelligence-Led Policing and public scrutiny

on research about the use of Intelligence-Led Policing to combat cybercrime as indicated in section 7.2.4. Underlying the fear of some people on the abuse of intelligence is the misuse of such intelligence by the police. This links to the above sentiment by the police that Intelligence-Led Policing is a subterfuge, thus making it more understandable why the general public should be worried about the use of Intelligence-Led Policing because they might to a larger extent suffer more from the abuse of this concept.

For the public to understand the regulated use of Intelligence-Led Policing in police operation, the police should work together with communities, businesses and security agencies to recognise the benefits of the end product of intelligence gathering to the successful operations of the police in the fight against cybercrime. It should also be noted that the success of Intelligence-Led Policing also requires support from the general public. As for the misuse of gathered intelligence by the police, the public should be encouraged to report such acts to the Inspector-General of Intelligence. As indicated in the previous section, the role of the Inspector-General of Intelligence is, among others, to monitor compliance of the security institutions with the constitution and applicable laws, reviewing the intelligence and counter-intelligence activities of these security agencies, and the reception and investigation of complaints from members of the public and members of these security institutions in terms of section 7(7) of the Intelligence Services Oversight Act 40 of 1994.

8.2.4 Investigation Licences

The delay in renewing expired licences to investigate cybercrime is another challenge that hampers the effective and efficient policing of cybercrime as indicated in section 7.2.6. It is clearly emphasised that without these licences, investigators cannot get access to all the functionalities of forensic tools, thus they have limited access to the data or evidence. To address this matter, the South African Police Service and Directorate for Priority Crime Investigation should enter into an automatic renewal of licences with the involved companies.

The licence should only cease to be operative once the automatic renewal contract is cancelled 6 months prior to its expiry date because it is clear that the time taken to renew expiring licence has a negative effect on the functioning of cybercrime

investigators. The need of these licences by investigators will remain an inherent essential resource in the successful resolution of cybercrime. Without these licences the investigators do not get access to all functionalities of forensic tools that enable them to gather and analyse digital evidence that is crucial for the successful resolution and prosecution of cybercrime.

8.2.5 Hidden Identities

The sophistication of cybercrime offenders to hide their identities and use other people's identities during the commission of cybercrime is indicated as a major difficulty in the investigation of this crime in section 7.2.6. Various measures that could mitigate this are computer forensics, cyber intelligence and artificial intelligence that can help to identify hidden information, files that are encrypted and to retrieve deleted information. Cybercrime investigation requires a combination of computer forensics, cyber intelligence and artificial intelligence software to help the investigators in the identification, collection, preservation and analysis of digital evidence from electronic devices. Computer forensic software has capabilities to gain access and identify information that is invisible like deleted or hidden information to help investigators to recover all digital evidence that are hanging on sophisticated network system.

8.2.6 Unwillingness to Testify

As indicated in section 7.2.6, some cybercrime victims are unwilling to testify, fearing to lose their clients and wanting to protect the reputation of their companies and this has a serious effect on successful prosecution. To deal with this unwillingness in order to enhance the successful prosecution of cybercriminals, investigators need to protect, support, advise and give assurance to the victims of cybercrime about the importance of cyber cases and the successful prosecution that will deter other potential cybercriminals from involving themselves in such activities. This will remove the sense of impunity and send a strong signal to potential cybercriminals that even if they are to succeed in committing such crime, they will ultimately be prosecuted and punished for it. One has to take note that the sense of impunity does not deter people from committing crime because they will know that once they are successful in committing crime then nothing will happen to them.

8.2.7 Cybercrime Strategy

As indicated in section 7.2.10 participants do not have a clear understanding of the difference between the legislation and the strategy of dealing with cybercrime. This situation has a profound impact on the combating, prevention and investigation of cybercrime because members who are at the forefront of dealing with cybercrime lacks knowledge and understanding of the difference between legislation and strategy. This could impact on the direction, guidelines and the procedure that they need to adhere to in dealing with rampant cybercrime. The South African Police Service and the Directorate for Priority Crime Investigation need to establish anti-cybercrime strategies that could guide cybercrime investigators in the detection, prevention and investigation of cybercrime. Such an anti-cybercrime strategy could also inform the increased visibility of the police in digital space to proactively detect and tackle cybercrime.

8.3 CONCLUSION

The aim of this study was to explore the use of Intelligence-Led Policing to combat cybercrime in South Africa. A literature review and empirical research were conducted to answer the research question and achieve the research objectives of the study. Cybercrime categories were explored to identify the challenges encountered by the police in combating this crime as well as the impact of those challenges to police operations. Despite the challenges encountered by the police in using Intelligence-Led Policing to combat cybercrime as indicated in this study, the value of the use of Intelligence-Led Policing forms a golden thread in all successful police operations.

The study covered national and international perspectives on the use of Intelligence-Led Policing by police agencies and make recommendations that could address the encountered challenges. It highlights specific findings that are thematically categorised as: the role of Intelligence-Led Policing in the investigation of cybercrime; investigative skills required in the investigation of cybercrime; the use of Intelligence-Led Policing by the South African Police Service to combat cybercrime; challenges encountered in using Intelligence-Led Policing to combat cybercrime; addressing challenges encountered in using Intelligence-Led Policing to combat cybercrime; challenges encountered in the investigation of cybercrime; the impact of the challenges encountered in the investigation of cybercrime; addressing the challenges encountered in the investigation of cybercrime; the strategy of the South African Police

Service in the investigation of cybercrime; the strategy of the Directorate for Priority Crime Investigation in the investigation of cybercrime; and the value of using Intelligence-Led Policing in the investigation of cybercrime in South Africa.

The findings revealing the accomplishment of the research objectives are contained in the themes that relate to the use of Intelligence-Led Policing by the South African Police Service to combat cybercrime, the challenges encountered in using Intelligence-Led Policing to combat cybercrime, and on the value of using Intelligence-Led Policing in the investigation of cybercrime in South Africa. The findings clearly indicate that there are challenges that need to be addressed in the effective and efficient use of Intelligence-Led Policing to combat crime and cybercrime in particular. The answers of the research questions are addressed in the theme that relates to the use of Intelligence-Led Policing by the South African Police Service to combat cybercrime, as well as in the theme that relates to the challenges encountered in using Intelligence-Led Policing to combat cybercrime.

The study concludes by suggesting recommendations to address the identified shortcomings in the use of Intelligence-Led Policing to fight crime. The recommendations on the conceptual implementation of Intelligence-Led Policing; misconception on Intelligence-Led Policing; lack of resources, training and fear; investigation licences; and hidden identities are all developed to address challenges encountered in the use of Intelligence-Led Policing to combat cybercrime. The last recommendation deals with the need to have a police strategy in the fight against cybercrime that could synchronise and synergise police activities in this regard.

LIST OF REFERENCES

- Abiodun, O.P. (2020). *Exploring the influence of organisational, environment and technological factors on information security policies and compliance at South African higher education institutions: Implications for biomedical research*. Cape Town: University of the Western Cape.
- Ajayi, E.F.G. (2016). Challenges to enforcement of cybercrimes laws and policy. *Journal of Internet and Information System*, 6 (1): 1-12.
- Akdemir, N., Sungur, B. & Basaranel, B.U. (2020). Examining the challenges of policing economic cybercrime in the UK. *International Security Congress, Special Issues*, 8(1): 113-134.
- Alkaabi, A.O.S. (2010). *Combating computer crime: An international perspective*. Unpublished Doctoral Thesis. Australia, Toowoomba City: University of Southern Queensland.
- Arnes, A. (2018). *Digital forensic*. (1st edition). West Sussex: John Wiley and Sons.
- Aphane, M. & Mofokeng J. (2021). South African police service capacity to respond to cybercrime: Challenges and potentials. *Journal of Southwest Jiaotong University*, 56(4): 165-186.
- Arquilla, J. & Ronfeldt, D. (2013). *The future of terror, crime and militancy: Networks and netwars*. Pittsburg: Rand Publications.
- Australian High-Tech Crime Centre. (2007). Technology enabled crime types: Counter intrusion and denial of service. Retrieved from: http://www.ahtcc.gov.au/tech/crimetypes/computer_intrusion.htm (Accessed on 17 February 2008).
- Babbie, E. & Mouton, J. (2012). *The Practice of Social Research*. (12th edition). Cape Town: Oxford University Press.
- Babbie, E. & Mouton, J. (2010). *The practice of social research*. (11th edition). Johannesburg: Oxford University Press.
- Baker, E.O. (2012). *Crime and public policy*. (7th edition). Belmont: Wadsworth.
- Barker, R.L. (2003). *Social work dictionary*. (5th edition). Washington DC: NASW.
- Basdeo, V., Montesh M. & Lekubu, B.K. (2014). Search for and seizure of evidence in cybercrime environment: A law-enforcement dilemma in South Africa criminal procedure. *Journal of Law, Society and Development*, 1(1): 48-67.
- Bernard, H.R. (2013). *Social research methods: qualitative and quantitative approaches*. (2nd edition). New Delhi: Sage.
- Berning, J. & Masiloane, D. (2012). The use of modus operandi forms by the South African Police Service to analyse crime. *Acta Criminologica*, 25(1):83-90.
- Bezuidenhout, C. (2008). The nature of police and community interaction alongside: The dawn of Intelligence-Led Policing. *Acta Criminologica: Crimsa Conference Special Edition*, 3: 48-67.
- Blaikie, N. & Priest, J. (2019). *Designing social research*. (3rd edition). Medford, MA: Polity Press.

- Bless, C., Higson-Smith, C. & Sithole, S.L (2013). *Fundamentals of research methods*. (5th edition). Cape Town: Juta.
- Boba, R.L. (2001). *Introductory guide to crime analysis and mapping*. New York: Community Oriented Policing Service US Department of Justice.
- Bogopa, T.J. (2020). Analysing cyber-bomb threats in South Africa. *Just Africa*, 5(2): 6-11.
- Boyd, A. (2014). How to detect an insider threat. Federal Times, 17 September 2014. Available at: <http://www.deferaltimes.com/article/20140917/cyber/309100024/how-detect-an-insider-threat> (Accessed on 20 September 2014).
- Brants, C, Jackson, A. & Wilson, T.J. (2020). A comparative analysis of Anglo-Dutch approaches to cyber policing: Checks and balances fit for purpose? *The Journal of Criminal Law*, 84(5): 451-457.
- Britz, M. (2013). *Computer forensic and cybercrime: An introduction*. (3rd edition). Delhi: Pearson.
- Buckley, J. (2014). *Managing intelligence: A guide for law enforcement professionals*. New York: Taylor & Francis Group.
- Budhram, T. (2016). Intelligence –Led policing: A grand narrative. *Acta Criminologica*, 29(1): 80-96.
- Buono, L. (2012). Gearing up the fight against cybercrime in the European Union: A new set of rules and the establishment of the European Cybercrime Centre (EC3). *New Journal of European Criminal Law*, 3 (3-4): 332-343.
- Burcher, M. & Whelan, C. (2019). Intelligence-Led Policing in practice: Reflection from intelligence analysts. *Police Quarterly*, 22(2):139-160.
- Bureau of Justice Assistance. (2014). Reducing crime through intelligence-led policing. United States of America: United States Department of Justice.
- Bureau of Justice Assistance. (2008). Reducing crime through Intelligence-Led Policing. Available at <https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/ReducingCrimeThroughILP.pdf>. (Accessed on 26 October 2020).
- Canaday, J. (2017). How the democratization of technology enhances Intelligence-Led policing and serves the community. Unpublished Masters Dissertation. Monterey: Naval Postgraduate School.
- Carter, J.G. (2016). Institutional pressures and isomorphism: The impact on Intelligence-Led Policing adoption. *Police Quarterly*, 19(4): 435-460. Retrieved from <https://doi.org/10.1177/1098611116639536> (Accessed on 21 March 2016).
- Carter, J.G. (2013). *Intelligence-Led Policing: A policing innovation*. El Paso: LFB Scholarly Publishing LLC.
- Carter, D.L & Carter, J.G. (2009). Intelligence-Led Policing conceptual and function considerations for public policy. *Criminal Justice Review*, 20(3):310-325.
- Carter, J.G. & Fox, B. (2018). Community policing and Intelligence-Led Policing: An examination of convergent or discriminant validity. *Policing: An International*

Journal of Police Strategies and Management. Retrieved from <https://doi.org/10.1108/PIJPSM-07-2018-0105> (Accessed on 13 December 2018).

- Casey, E. (2011). *Digital evidence and computer: Forensic Science, computers*. New York: Elsevier.
- Cassim, F. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves? *Potchefstroom Electronic Law Journal*, 18(2): 68-110.
- Cassim, F. (2012). Addressing the spectre of cyber terrorism: A comparative perspective. *Potchefstroom Electronic Law Journal*, 15 (2): 381-415.
- Cassim, F. (2009). Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study. *Potchefstroom Electronic Law Journal*, 12 (4): 36-78.
- Chainey, S. (2012). Improving the explanatory content analysis products using hypothesis testing. *Journal of Policy and Practice*, 6(2): 108-121.
- Champion, D.J. (2001). *Correction in the United States: A contemporary perspective*. 3rd edition. New Jersey: Upper Saddle River.
- Chan, N., Coronel, S. & Ong, Y, C. (2003). The threat of the cybercrime Act 2001 to Australia IT professionals, in proceedings of the first Australian Undergraduate Students Computing Conference. Retrieved from: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.4.3391&rep1&type=pdf>. (Accessed on 13 December 2018).
- Chitimira, H. & Ncube, P. (2021). The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financial crime in South Africa banks. *Potchefstroom Electronic Law Journal*, 24(1):1-33.
- Cichoracki, C. (2020). The effectiveness of Intelligence-Led Policing in countering terrorism on global, national and cyber fronts. Unpublished Masters Dissertation, Baltimore: Johns Hopkins University.
- Civilian Secretariat for Police. (2013). *Green Paper on Policing*. Pretoria: Government Printer.
- Clark, R.V. (2004). Technology, criminology and crime science. *European Journal on Criminal Policy and Research*, 7(1):3-7.
- Clough, J. (2010). *Principles of cybercrime*. New York: Cambridge University Press.
- Clough, D. & Nutbrown, C. (2012). *A student's guide to methodology*. (3rd edition). London: Sage.
- Constitution of the Republic of South Africa. (1996). Republic of South Africa. Pretoria: Government Printers.
- Cornish, D.B. (2011). *The procedural analysis of offending and its relevance for situational prevention: In crime prevention studies*. Monsey, NJ: Criminal Justice Press.

- Cowan, D., Burton, C. & Moreto, W. (2018). Conservation-based intelligence-led policing: An intra-organizational interpersonal examination. *An International Journal of Policing*. Retrieved from www.emeraldinsight.com/1363-951xhtm (Accessed on 26 November 2018).
- Creswell, J.W. (2014). *Research design: Qualitative, quantitative and mixed methods approaches*. (4th edition). California: Sage.
- Creswell, J.W. (2013). *Qualitative, quantitative and mixed methods approaches*. (3rd edition). Los Angeles: Sage.
- Creswell, J.W. (2009). *Research design: Qualitative, quantitative and mixed methods approaches*. (2nd edition). New Delhi: Sage.
- Creswell, J.W. & Clark, V.L.P. (2018). *Designing and conducting mixed methods research*. (3rd edition). New Delhi: Sage.
- Creswell, J. W. & Creswell, J. D. (2018). *Research design: Qualitative, quantitative and mixed methods approaches*. (5th edition). New Delhi: Sage.
- Darroch, S. & Mazerolle, L. (2013). Intelligence-Led Policing: A comparative analysis of organisational factors influencing innovation uptake. *Police Quarterly*, 16(1): 3-37.
- Das, S. & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Sciences and Emerging Technology*, 6(2): 142-153.
- Davenport, T.H., & Prusak, L. (1998). Working knowledge: How organizations manage what they know. Retrieved from <http://www.acm.org/ubiquity/book/t-ubiquity/book/t-davenport-1.html> (Accessed on 30 January 1998).
- David, T. & Hodges, I.D. 2010. *Designing and managing your research project: Core skills for social and health research*. Thousand Oaks, CA: Sage.
- Davies, M. & Hughes, N. (2014). *Doing a successful research project: Using qualitative or quantitative methods*. (2nd edition). New York: Palgrave Macmillan.
- Dawson, C. 2016. *100 Activities for Teaching Research Methods*. London: Sage.
- Decock, N. (2004). Managing the police patrol time, the role of supervisors and detectives. *Justice Quarterly*, 22(4): 23-65.
- Deflem, M. & Maybin, L.C. (2005). *Interpol and the policing of international terrorism: Developments and dynamics since September 11*. New Jersey: Prentice Hall.
- Denscombe, M. (2010). *Ground rules for social research: Guideline for good practice*. (2nd edition). New York: Open University Press.
- Denscombe, M. (2007). *The good research guide: For small scale social research projects*. (3rd edition). New York: McGraw-Hill.
- Department of Justice, South Africa. (1994). Act No. 40 of 1994: Intelligence Services Oversight. *Government Gazette*, 354(16129). Pretoria: Government Printers. 02 December.

- Department of Justice, South Africa. (1999). Act No. 38 of 1999: Prevention of Organised Crime Second Amendment. *Government Gazette*, 411(20447). Pretoria: Government Printers. 07 September.
- Department of Justice, South Africa. (2021). Act No. 19 of 2020: Cybercrimes Act 19 of 2020. *Government Gazette*, 324(44651). Pretoria: Government Printers. 01 June.
- Desai, A. (2018). Cybercrime, cyber-surveillance, state surveillance in South Africa. *Act Criminologica*, 31 (3): 149-160.
- De Vos, A.S., Strydom, H., Fouche, C.B. & Delpont, C.S.L. (2012). *Research at grass roots for the social science and human science professions*. (4th edition). Pretoria: Van Schaik.
- De Vos, S.A., Strydom, H., Fouche, C.B. & Delpont, C.S.L. (2011). *Research at grass roots for the social sciences and human service professions*. (3rd edition). Pretoria: Van Schaik Publishers.
- De Vos, A.S., Strydom, H., Fouche, C.B. & Delpont, C.S.L (2005). *Research at grass roots for the social science and human science professions*. (2nd edition). Pretoria: Van Schaik.
- Dlamini, S. & Mbambo, C. (2019a). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Journal of Cogent Social Science*, 5(1): 1-13.
- Dlamini, S. & Mbambo, C. (2019b). An exploratory study on mechanisms in place to combat hacking in South Africa: A criminological perspective. *American Journal of Humanities and Social Science Research*, 3(1):146-154.
- Du Preez, N. & Muthaphuli, P. (2019). The deterrent value of punishment on crime prevention using judicial approaches. *Just Africa*, 2019(1): 34-36.
- Du Toit, R., Hadebe, P.N. & Mphatheni, M. (2018). Public perception of cybersecurity: A South African context. *Acta Criminologica*, 31(3):111-131.
- Easttom, C. & Taylor, D.J. (2011). *Computer crime, investigation and the law*. Boston, MA: Cengage Learning.
- Edward, G. (2019). *Cybercrime investigators handbook*. New Jersey: John & Sons.
- Eiselen, S. (2014). Fiddling with the ECT ACT- Electronic Signatures. *Potchefstroom Electronic Law Journal*, 17(6): 2805-2820.
- Electronic Communications and Transactions Act No 25 of 2002. Republic of South Africa. Pretoria: Government Printers.
- Evans, R.M. (2012). The diamond matrix: A science-driven approach to policing with crime intelligence. *Policing: A Journal of Policy and Practice*, 6(2):133-143.
- Ezeji, C.L. & Olutola, A.A. (2018). The use of Intelligence-Led Policing in combating technology-based crimes in South Africa. *Journal of African Foreign Affairs*, 5(2): 167-188.

- Ezeji, C.L., Olutola, A.A. & Bello, P.O. (2018). Cyber-related crime in South Africa: Extent and perspective of state's role-players. *Acta Criminologica*, 31(3): 93-110.
- Ezeji, C.L. (2017). Overview of Intelligence-Led Policing and crime prevention in South Africa. Unpublished Doctoral thesis. Pretoria: Tshwane University of Technology.
- Ezeji, C.L. (2014). Combating cyber related crime in South Africa. Unpublished Masters Dissertation. Pretoria: Tshwane University of Technology.
- Federal Bureau of Investigation. (2020). Federal Bureau of Investigation Cybercrime Strategy. Available at www.fbi.gov. (Accessed on 07 July 2023).
- Fick, J. (2019). Taking the fight to the criminals- An intelligence-guided approach to cybercrime investigation. *Servamus Community-based Safety and Security Magazine*, 112: 20-32.
- Financial Intelligence Centre Act 38 of 2001. Republic of South Africa. Pretoria: Government Printers.
- Fink, A. 2010. *Conducting research literature from internet to paper*. 3rd edition. Los Angeles Sage.
- Flick, U. (2014). *Introducing research methodology: A beginner's guide to doing a research project*. London: Sage.
- Flick, U. (2011). *Introducing research methodology: A beginner's guide to doing a research project*. London: Sage.
- Flood, B. & Gaspar, R. (2009). *Strategic aspects of the UK National Intelligence Model: In Strategic Thinking in Criminal Intelligence*. (2nd edition). Sydney: Federation Press.
- Fraenkel, J.R., Wallen, N.E. & Hyun, H.H. (2015). *How to design and evaluate research in education*. (9th edition). New York: McGraw-Hill Education.
- Franklin, M.I. (2012). *Understanding research: Coping with the qualitative divide*. New York: Routledge.
- Geldenhuys, K. (2017). Online child pornography- A never-ending story. *Servamus Community-based Safety and Security Magazine*, 110 (05): 21-27.
- Gemke, P., Den Hengst, M., Van Rosmalen, F. & De Boer, A. (2021). Towards a Maturity model for Intelligence-Led Policing: A case study research on the investigation of drugs crime and on football and safety in the Dutch police. *An International Journal Police Practice and Research*, 22 (1): 190-207. <https://doi.org/10.1080/15614263.2019.1689135>.
- Gibbs, C., McGarrell, E.F. & Sullivan, B. (2015). Intelligence-Led Policing and transnational environmental crime: A process evaluation. *European Journal of Criminology*, 12(2):242-259.
- Gills, P. (2013). *Organised crime in Companion to intelligence studies*. Oxford: Routledge.

- Goldstein, H. (2003). *The future development of problem-oriented policing, the most critical need*. Monsley, NJ: Criminal Justice Press.
- Govender, D. (2012). Information management strategies to combat crime and prevent losses. *Acta Criminologica*, 25(1): 79-96.
- Govender, D. (2011). Problems experienced by detectives in the processing and utilisation of crime information at the Rustenburg detective unit, North-West Province, South Africa. *Acta Criminologica*, 24(2): 112-129.
- Gray, D.E. (2018). *Doing research in the real world*. 4th edition. New Delhi: Sage.
- Grazioli, A.M. & Jarvenpa, J. (2013). *Information about phishing methods*. New York: Harper Collins.
- Gumbi, D. (2018). Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT Legislative Framework of South Africa, Kenya, India, the United States and United Kingdom. Unpublished Masters Dissertation. Cape Town: University of Cape Town.
- Guthrie, G. (2010). *Basic research methods: An entry to social science research*. (3rd edition). Los Angeles: Sage.
- Harding, J. (2013). *Qualitative data analysis from start to finish*. Los Angeles: Sage.
- Harfield, C. & Kwewen, C. (2008). The paradigm pathologies and practicalities policing organised crime in England and Wales. *Policing Journal of Policy and Practice*, 2(1): 63-73.
- Heldon, D. (2002). *Security informatics in the first 21st century*. Upper Saddle River: Prentice Hall.
- Herhalt, J. (2011). Cybercrime: A growing challenge for government, KPMG Issues Monitor, 8:1-24. <https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cybercrime.pdf>. (Accessed on 26 March 2014).
- Hesse-Biber, S.N. & Leavy, P. (2011). *The practice of qualitative research*. (2nd edition). California: Sage.
- Heuer, R.J. (2009). *The evolution of structured analytic techniques*. Paper presented to the National Academy of Science, National Research Council Committee on Behavioural and Social Science Research to Improve Intelligence Analysis for National Security. Washington, DC, December 8.
- Hill, B. & Paynich, R. (2014). *Fundamentals of crime mapping*. (2nd edition). Burlington: Jones and Bartlett Learning.
- Holt, T.J. & Bossler, A.M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, 29(4): 420-436.
- Holt, T.J., Burruss, G.W. & Bossler, A.M. (2018). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology*, 62(6): 1720-1741.
- Holt, T.J., Navarro, J.N. & Shelly, C. (2020). Exploring the moderating role of gender

- In juvenile hacking behaviours. *Crime and Delinquency*, 66(11): 1533-1555.
- Horne, J.S. (2009). Crime information analysis within a public service organization: An assessment. *Acta Criminologica*, 22(1): 68-80.
- Hussien, A.A. (2021). Cyber security crimes, ethics and a suggested Algorithm to overcome cyber-physical systems problems (CybSec1). *Journal of Information Security*, 12: 56-78.
- International Telecommunication Union (2012). Understanding cybercrime: Phenomena, challenges and legal response. A report of understanding cybercrime: A guide for developing countries. Available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.Html. (Accessed on 16 September 2022).
- Irons, A & Ophoff, J. (2016). Aspects of digital forensics in South Africa. *Interdisciplinary Journal of Information, Knowledge, and Management*, 11: 273-283.
- Jackson, J.E. (2012). *Information security management handbook*. Boston: Abcon.
- Jensen, C.J., Regens, J.M., & Griffin, N. (2013). Intelligence-Led Policing as a tool for countering the terrorism threat. *The Homeland Security Review*, 7:265-283.
- Jesson, J.K., Matheson, L., & Lacey, F.M. (2011). *Doing your literature review: Traditional and systematic techniques*. London: Sage.
- Jideani, P.C. (2018). Towards a cyber-security framework for South Africa E-Retail organisations. Unpublished Masters Dissertation. Cape Town: Cape Peninsula University of Technology.
- Jones, G.M. & Winster, W. (2017). Forensic analysis on Smart phones using mobile forensic tools. *International Journal of Computational Intelligence Research*. 13(8): 1859-1869.
- Jonker, D.C. (2011). The role of the department of correctional services in the rehabilitation of child molesters. Unpublished Masters Dissertation. Pretoria: Unisa.
- Kader, S. & Minnaar, A. (2015). Cybercrime investigation: Cyber-processes for detecting of cybercriminal activities, cyber-intelligence and evidence gathering. *Acta Criminologica*, 5: 67-81.
- Kelly, A. & Finlayson, A. (2015). Can Facebook save neighbourhood watch? *The Police Journal*, 88(1):65-77.
- Kempen, A. (2020). Are all hackers bad? *Servamus Community-based Safety and Security Magazine*, 113 (06): 1-2.
- Kempen, A. (2019). Cybercrime knows no borders. *Servamus Community-based Safety and Security Magazine*, 112 (8): 50-54.
- Kempen, A. (2017). South Africa and France to fight cybercrime together. *Servamus Community-based Safety and Security Magazine*, 110(08): 59-59.
- Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, 30(4): 470-486.

- Kim, M.W. (1997). How countries handle computer crime. Paper for MIT 6.805/STS085: Ethics and law on the electronic frontier. Available at <https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/kim-crime.html>. (Accessed on 17 February 2008).
- Kleiven, M. (2005). Where's the intelligence in the UK's National Intelligence Model? London: University of Portsmouth.
- Kopelev, S. (2000). Cracking computer codes. *Law Enforcement Technology*, 27(1): 60-67.
- Koziarski, J. & Lee, J.R. (2020). Connecting evidence based policing and cybercrime. *Policing: An International Journal*, 43(1):1-23.
- Krause, A. (2007). The crime threat analysis process- An assessment. Unpublished Masters Dissertation. Pretoria: Unisa.
- Kumar, R. (2014). *Research methodology. A step-by-step guide for beginners*. (4th edition). London: Sage.
- Kumar, R. (2011). *Research methodology as step-by-step guide for beginners*. (3rd edition). California: Sage.
- Kumar, R. (2005). *Research methodology: A step-by-step guide for beginners*. London: Sage.
- Kundi, G.M. & Akhtar, R. (2014). Digital revolution, cybercrimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications*, 04 (04): 61-70.
- Labane, A. (2012). Offender classification as a rehabilitation tool. Unpublished Masters Dissertation. Pretoria: Unisa.
- Lambrechts, D. (2021a). The Cybercrime Act 19 of 2020. A legal discussion: Part 1. *Servamus Community-based Safety and Security Magazine*, 114(10): 38-43.
- Lambrechts, D. (2021b). The Cybercrime Act 19 of 2020. A legal discussion: Part 2. *Servamus Community-based Safety and Security Magazine*, 114(11): 22-29.
- Lanier, M.M. & Briggs, L.T. (2014). *Research methods in criminal justice and criminology a mixed methods approach*. New Delhi: Oxford University Press.
- Leedy, P.D & Ormrod, J.E. (2016). *Practical research: Planning and design*. (12th edition). Essex: Pearson.
- Leedy, P.D. & Ormrod, J.E. (2015). *Practical research. Planning design*. (11th edition). Boston, MA: Pearson.
- Leedy, P.D. & Ormrod, J.E. (2014). *Practical research: Planning and design*. (10th edition). New Jersey: Pearson Upper Saddle River.
- Leedy, P.D. & Ormrod, J.E. (2013). *Practical research: Planning and design*. (9th edition). Boston: Pearson Education.
- Leedy, P.D. & Ormrod, J.E. (2001). *Practical research: Planning and design*. (7th edition). New Jersey: Merrill Prentice Hall.

- Lesion, I. (2012). Towards efficient and equity in law enforcement Rachel law and the protection of drug informants. *Boston College Journal of Law and Social Justice*, 32 (2): 391-419.
- Levi, M. & Maguire, M. (2012). *Something old and something new, something not entirely blue in policing, politics, culture and control*. Oxford: Hart Publishing.
- Lewis, C. (2011). *Criminal justice statistic collected by international agencies*. Portsmouth: Portsmouth University Press.
- Majesty's Inspectorate of Constabulary. (2014). Crime recovering making the victim counts. London: Majesty's Inspectorate of Constabulary.
- Makkai, T., Ratcliffe, J.H. & Lisa, C. (2004). Act of recidivist offenders. *Research and Public Policy*, 4(2): 54-83.
- Mandia, K. (2011). *Incident response investigating computer crime*. Osborne, CA: McGrawHil Press.
- Maras, M.H. (2015). *Computer forensic: Cybercriminals, Laws and Evidence*. (2nd edition). Burlington, MA: Jones and Bartlett learning.
- Marshall, C. & Rossman, G.B. (2011). *Designing qualitative research*. (5th edition). New Delhi: Sage.
- Mashiloane, N.P. (2014). The use of Intelligence-Led Policing in crime prevention by South African Police Service. Unpublished Doctoral thesis. Pretoria: Unisa.
- Matsaung, P.M. (2019). The value of crime mapping in crime prevention. Unpublished Masters Dissertation. Pretoria: Unisa.
- May, T. (2011). *Social research: issues, methods and process*. (3rd edition). New York: Open University Press.
- Meyer, S. (2013). *Impending lone wolf. Lesson derived from 2011 Norway attack crime scene*. Norway: Norway Justice Department.
- McMurdie, C. (2016). The cybercrime landscape and our policing response. *Journal of Cyber Policy*, 1(1):85-93.
- McNeal, S.L., Kunkle, S.M. & Schemeida, M. (2018). Cyber harassment and policy reform in the digital age: Emerging research and opportunities. Hershey, PA: IGI Global.
- Mills, J. & Birks, M. (2014). *Qualitative methodology: A practical guide*. London: Sage.
- Minnaar, A. (2020). Gone phishing: The cynical and opportunistic exploitation of the corona virus pandemic by cybercriminals. *Acta Criminologica*, 33(3): 28-53.
- Minnaar, A. (2016). Organised crime and the new more sophisticated criminals within the cybercrime environment: How organised are they in the traditional sense? *Acta Criminologica*, 29(2): 123-140.
- Minnaar, A. (2014). Crackers, cyber-attacks and cyber-security vulnerabilities: The difficulties in combating new cybercriminals. *Acta Criminologica*, Special Edition, No 2: 127-144).

- Minnaar, A. (2013). Information security, cybercrime, cyber-terrorism and the exploitation of cyber-security vulnerabilities. *Act Criminologica*, 26 (2): i – iv.
- Mngadi, W.B. (2021). An analysis of cybercrime investigation by Directorate for Priority Crime Investigation. Unpublished Masters Dissertation. Pretoria: Unisa.
- Modi, S.N. (2016). Role of Trustmark in E-commerce. *International Journal for Innovations in Engineering, Management and Technology*, 1(1):35-40.
- Montesh, I.P. (2019). The challenges facing members of the South African Police Service in peacekeeping missions in Africa. Unpublished Doctoral thesis. Pretoria: Unisa.
- Moore, R. (2015). *Cybercrime: Investigating high-technology crime*. (2nd edition). New York: Routledge.
- Moskowitz, S.L. (2017). Cybercrime and business strategies for global corporate security. Kidlington, Oxford: Butterworth-Heinemann.
- Mothibi, A. & Amali, S.E. (2018). Curbing cybercrime at institution of higher learning: A case study of the Information Communication Technology Unit at selected South African Universities. *Acta Criminologica*, 31(3): 57-70.
- Mpuru, L. (2017). Cyber security concerns in South Africa: Current Legislature. *Servamus Community-based Safety and Security Magazine*, 110(12): 44-45.
- Mugari, I., Maunga, M. & Chigariro, T. (2015). Embracing Intelligence-Led Policing in the Republic of Zimbabwe. *International Journal of Innovative Research and Development*, 4(2):87-94.
- Muthaphuli, P. (2012). Crime prevention and sentencing: A practical penological perspective. Unpublished Doctoral Thesis. Pretoria: Unisa.
- Myeza, N.W. (2019). An analysis of the prosecution-led investigation model in murder cases. Unpublished Masters Dissertation. Pretoria: Unisa.
- National Institutes of Justice. (2001). Electronic crime scene investigation: A guide for first responders. Available at <http://www.ncjrs.gov/pdffiles1/nij/187736.pdf> (Accessed on 08 April 2001).
- National Institutes of Standard and Technology. (2003). Computer forensic tool testing project overview. Available at <http://www.cftt.nist.gov/projectoverview.htm> (Accessed on 15 January 2008).
- National Strategic Intelligence Act No 39 of 1994. Republic of South Africa. Pretoria: Government Printers.
- Ndaba, V. (2013). Computer seizure as techniques in forensic investigation. Unpublished Masters Dissertation. Pretoria: Unisa.
- Nduka, R.E. & Basdeo, V. (2021). The need for harmonised and specialised global legislation to address the growing spectre of cybercrime. *Southern African Public Law*, 36(2): 1-22.
- Newburn, T. (2003). *Handbook of policing*. Devon: Willan Publishing.

- Newman, I. & Covrig, D.M. (2013). Writer's Forum — Building consistency between title, problem statement, purpose, & research questions to improve the quality of research plans and reports. *New Horizons in Adult Education & Human Resource Development*, 25 (1) 70-79.
- Newman, I., Ridenour, C., Newman, C. & DeMarco, G.M.P. (2003). A typology of research purposes and its relationship to mixed methods research. In A. Tashakkori & C. Teddlie, (Eds.) *Handbook of mixed methods in social & behavioral research* (pp. 167-188). Thousand Oaks, CA: Sage.
- New Zealand Ministry of Justice (2019). The United Nation Convention. New Zealand: Foreign Affairs and Trade Department.
- Ntsabula, N. (2017). Cyber security and legislation in South Africa. Unpublished Masters Dissertation. Pretoria: University of Pretoria.
- Oliver, P. (2010). *The student's guide to research ethics*. New York: Open University Press.
- Ortmeier, P.J. (2013). *Introduction to security operations and Management*. (4th edition). Cape Town: Pearson Education.
- Osborn, N. (2012). To what degree have non-police public service adopted the National Intelligence Model? What benefits could be the National Intelligence Analysis? Washington DC: Joint Military College.
- Osborne, D.A. & Wernicke, S.C. (2003). *Introduction to crime analysis: Basic resources for criminal justice practice*. New York: Haworth Press.
- Pattern, M.L & Newhart, M. (2018). *Understanding research methods: An overview of the essentials*. 10th edition. New York: Routledge.
- Phahlamohlaka, J. and Hefer, J. (2019). The impact of Cybercrimes and Cyber Security Bill on South African National Security: An institutional theory analytic perspective. Available at <http://www.threatcon.co.za/2-2.html>. (Accessed on 13 November 2020).
- Punch, F.P. (2016). *Developing effective research proposal*. 3rd edition. London: Sage.
- Punch, K.F. (2005). *Introduction to social research: Quantitative and qualitative approaches*. (2nd edition). Los Angeles: Sage.
- Ratcliffe, J.H. (2016). *Intelligence-Led Policing*. (2nd edition). New York: Routledge.
- Ratcliffe, J.H. (2014). What is the future of predicting policing? *Journal of Transactional Criminology*, 20(1):40-45.
- Ratcliffe, J.H. (2008). Supplemental material for Intelligence-Led Policing. Available at http://tandfbis.s3.amazonaws.com/rt-edia/pdf/9781843923398/ilp_supplemental.pdf. (Accessed on 11 November 2020).
- Ratcliffe, J.H. (2007). *Integrated and crime intelligence and crime analysis enhancement information management for law enforcement leaders*. Washington DC: Police Foundation.

- Ratcliffe, J.H & Guiditti, A. (2008). State police investigation structure and the adoption of Intelligence-Led Policing. *An international Journal of Police Strategies and Management*, 31(1): 109-128.
- Ratcliffe, J.H. & Makkai, T. (2004). Diffusion of benefits, evaluating a policing operation. *Trend and Issues in Crime and Criminal Justice*, 278: 1-6.
- Reddy, E. & Minnaar, A. (2018). Cryptocurrency: A tool and target for cybercrime. *Acta Criminologica*, 31(1): 71-92.
- Reddy, E. & Minnaar, A. (2015). Safeguarding children from becoming victims of online sexual abuse facilitated by virtual worlds. *Child Abuse Research: A South African Journal*, 16 (1): 23-29.
- Regulation of Interception of Information Centre Act 70 of 2002. Government Gazette. Pretoria: Government Printer.
- Rehman, R., Hazarika, G.C... & Chetia, G. (2011). Malware threats and mitigation strategies: A survey. Available at www.jatit.org. (Accessed on 31 July 2011).
- Richardson, L. (2000). Evaluating ethnography. *Qualitative Inquiry*, 6: 253-256.
- Ritter, N. (2006). Digital evidence: How law enforcement can level the playing field with criminals. *National Institutes of Justice Journal*, 254:20-22.
- Robb, D. (2015). Whitepaper: Your money or your life files. Available at <https://www.netthreat.co.uk/assets/knowbe4/Your-Money-or-Your-Life-Files.pdf> (Accessed on 18 May 2022).
- Rolfe, G. (2004). Validity, trustworthiness and rigour: quality and the idea of qualitative research. *The Journal of Advanced Nursing*, 53 (3): 304-310.
- Ronckowski, M.R. (2012). *Terrorism and organised hate crime: Intelligence gathering, analysis and investigation*. (3rd edition). New York: Taylor and Francis.
- Roos, C.J. (2012). Governance responses to hacking in the banking sector of South Africa: An exploratory study. Unpublished Doctoral Thesis. Johannesburg: University of Johannesburg.
- Santos, R.B. (2013). *Crime analysis with crime mapping*. (3rd edition). Los Angeles: Sage.
- Scheepers, S.A. & Schultz, C.M. (2019). Organisational learning in crime intelligence: A qualitative review. *Journal of Contemporary Management*, 16(2):361-381.
- Schultz, C.B. (2016). Cybercrime: An analysis of current legislation in South Africa. Unpublished Masters Dissertation. Pretoria: University of Pretoria.
- Schultz, E.E. (2013). *Fighting malicious code*. New York: Elsevier.
- Scotland Police Authority. (2020). Cyber Strategy 2020: Keeping people safe in the digital world. Available at <https://www.scotland.police.uk/spa-media/msbpuuud/cyber-strategy.pdf> (Accessed on 07 July 2023).
- Siegel, L.J. (2013). *Criminology: Theories, patterns and typologies*. (11th edition). Wadsworth: Cengage Learning.

- Silverman, D. (2000). *Doing qualitative research: A practical handbook*. London: Sage.
- South Africa. (2016). Cybercrime and Cybersecurity Bill. Pretoria: Government Printers.
- South Africa. (2005). White Paper on Corrections in South Africa. Pretoria: Department of Correctional Services.
- Staff Writer. (2018). South Africans hit by massive Bitcoin scam. MyBroadBand. 01 March. Available at: <https://mybroadband.co.za/news/cryptocurrency/250893-South-Africans-hit-by-massive-bitcoin-scam.html> (Accessed on 20 February 2018).
- Stainer, I.P. (2013). Contemporary organizational pathologies in policing information sharing. Unpublished Doctoral Thesis. London: London Metropolitan University.
- Stallings, W. (2019). *Effective cyber-security: A guide to using best practices and standards*. Cape Town: Pearson Education.
- Stenton, A.E. (2006). Crime analysis: An examination of crime prevention and reduction strategies. Ottawa: Simon Frazer University.
- Stering, R.S. (2008). *Police officers handbook: An analytical and administrative guide*. Boston: Jones and Bartlett.
- Symantec Intelligence Reports. (2013). Information on cybercrime. Available at www.symantec.com (Accessed on 27 May 2013).
- Taherdoost, H. (2016). Sampling methods in research methodology: How to choose sampling technique for research. *International Journal of Academic Research in Management*, 5: 17-29.
- Tahir, R. (2018). A Study on malware and malware detection techniques. *International Journal of Education and Management Engineering*, 2: 20-30.
- Terre Blanche, M., Durreheim, K. & Painter, D. (2006). *Research in practice: Applied methods for social sciences*. 2nd edition. Cape Town: University of Cape Town.
- Tesch, R. (1990). *Qualitative research: Analysis types and software tools*. London: Falmer Press.
- Thenga, G. (2018). A critical analysis of the policing of counterfeit goods in South Africa. Unpublished Doctoral Thesis. Pretoria: Unisa.
- The Republic of South Africa. (2020). Cybercrime Act, No 19 of 2020. Government Gazette, No 44651, 1 June 2021. Cape Town: Government Printers.
- Townsley, M., Mann, M. & Garrett, K. (2012). The missing link of crime analysis: A systematic approach to testing competing hypotheses. *Policing: A Journal of Policy and Practice*, 5(2): 158-171.
- Tracy, S.J. (2013). *Qualitative research methods, collecting evidence, crafting analysis and communicating impact*. New York: John Wiley & Son.

- Tracy, S.J. (2010) Qualitative quality: Eight “Big Tent” criteria for excellent qualitative research. *Qualitative Inquiry*, 16(10): 837-851.
- Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies*, 18(4-5): 530-547.
- Unisa. (2013). Policy on research ethics. Available at www.unisa.ac.za.on-/Policy-Research-ethics-Rev-appr-Council. (Accessed on 10 October 2013).
- United Kingdom Computer Misuse Act of 1990. What is the Computer Misuse Act? Available at <https://www.itpro.co.uk/it-legislation/28174/what-is-the-computer-misuse-act>. (Accessed on 27 June 2022).
- United Kingdom’s Strategy for Counter-Terrorism. (2011). Available at <https://www.gov.uk/government/publications/counter-terrorism-strategy-contest>. (Accessed on 12 July 2021).
- United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. February. UNODC/UN: Vienna/New York.
- United Nations. (2004). *UN convention against transactional organised and the protocols thereto*. New York: United Nations.
- Urbas, G. (2012). Cybercrime, jurisdiction and extradition: The extended reach of cross-border law enforcement. *Journal of Internet Law*, 16(1): 8-17.
- US Department of Justice. (2008). Computer crime and intellectual property section: Reporting computer, internet-related or intellectual property crime. Available at <http://www.usdoj.gov/criminal/cybercrime/reporting.htm> (Accessed on 14 January 2008).
- US Government Accountability Office. (2014). Information security: Agencies need to improve cyber incident response practices. Available at <http://www.gao.gov/products/GAO-14-354> (Accessed on 15 July 2015).
- Van Graan, J. & Zinn, R. (2015). Child care institutions as a source of crime Intelligence in combating child sexual crimes. *Child Abuse Research: A South African Journal*, 16(1):40-54.
- Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. Available at <https://doi.org/10.239662/10539/23573>. (Accessed on 15 December 2017).
- Van Rensburg, S.J. (2018). Contextualising social engineering through criminological theorising. *Acta Criminologica*, 13 (3): 1-19.
- Veerasingam, N. (2017). Cyber threat intelligence exchange- A growing requirement. Proceedings of the 16th European Conference on cyber warfare and security. Dublin, Ireland. Available at <http://hdl.handle.net/10204/9662>. (Accessed on 29 June 2021).
- Vermaat, M.E., Sebok, S.L., Freund, S.M., Campbell, J.T. & Frudenberg, M. (2016). *Discovering computers 2016 essentials: Tools, apps, devices and the impact of technology*. Boston: Cengage Learning.

- Victoria Police. (2022). Cybercrime Strategy 2020 – 2027. Available at https://content.police.vic.gov.au/sites/default/files/2022-08/Victoria-Police-Cybercrime-Strategy-2022-2027.pdf#_ga=2.165277631.1663632996.1688720164-70056451.1686902998. (Accessed on 07 July 2023).
- Walker, T., Allen, K., Abderrahmane, A. & Yared, T. (2021). Balancing basic freedoms and the need to fight against cybercrime. *ISS Peace and Security Council Report*, 137:5-7.
- Walliman, N. (2016). *Social research methods*. (2nd edition). New Delhi: Sage.
- Wartell, J. & Gallagher, K. (2012). Translating environmental criminology theory into crime analysis practice. *Policing: A Journal of Policy and Practice*, 6(4): 377-387.
- Weatherburn, D. (2001). *Law and order in Australia rhetorical and reality*. Sydney: Federal Press.
- Welman, J.C, Kruger, S.J, & Mitchell, B. (2005). *Research methodology*. (3rd edition). Cape Town: Oxford University Press.
- Welman, J.C. & Kruger, S.J. (2001). *Research methodology*. (2th edition). Cape Town: Oxford University Press.
- White, V. & Goodman, P. (2021). Tackling cybercrime across the borders. *Servamus Community-based Safety and Security Magazine*, 114(10): 32-35.
- Widdsup, S., Spitter, M., Hylendem, D. & Basset, G. (2018). Verizon data breach. Investigation report. Available at <https://www.researchgate.net/publication/32445340-2018-verizon-data-breach-investigationreport> (Accessed on 06 November 2017).
- Willems, E. (2019). *Cyber danger: Understanding and guarding against cybercrime*. Switzerland: Springer Nature.
- Withrow, B.L. (2014). *Research methods in crime and justice*. London: Routledge.
- Wortley, R. & Mazerolle, L. (2008). *Environmental criminology and crime analysis*. Devon: Willan.
- Zinn, R. (2011). Inaugural Address. Pretoria: University of South Africa. Available at <http://www.saps.gov.za/dynamicModules> (Accessed on 27 August 2013).
- Zinn, R. (2010). Inside information: Sourcing crime intelligence from incarcerated house robbers. *South African Crime Quarterly*, 32: 27-35.

ANNEXURE A: INTERVIEW SCHEDULE OF DETECTIVES

1. What is the role of Intelligence-Led Policing in the investigation of cybercrime?

.....
.....
.....
.....
.....
.....

2. Which investigative skills are required for one to investigate cybercrime effectively?

.....
.....
.....
.....
.....
.....

3. What are the challenges encountered in the investigation of cybercrime?

.....
.....
.....
.....
.....
.....

3.1 What is the impact of those challenges in successful investigation?

.....
.....
.....
.....
.....
.....

3.2 How can such challenges be addressed?

.....
.....
.....
.....
.....
.....

4. Does the South African Police Service have a focused strategy that deals with cybercrime investigation?

.....
.....
.....
.....
.....
.....

4.1 If the answer to the above question is yes, how effective is such strategy?

.....
.....
.....
.....
.....
.....

5. What is the value of using Intelligence-Led Policing to investigate cybercrime in South Africa?

.....
.....
.....
.....
.....
.....

ANNEXURE B: INTERVIEW SCHEDULE OF CRIME INTELLIGENCE

1. How is the Intelligence-Led Policing used by the SAPS to combat cybercrimes?

.....
.....
.....
.....
.....

2. How can Intelligence-Led Policing be used by the South African Police Service in combating cybercrime?

.....
.....
.....
.....
.....

3. What is the value of using Intelligence-Led Policing in combating cybercrime?

.....
.....
.....
.....
.....

4. What are challenges encountered in using Intelligence-Led Policing to combat cybercrime?

.....
.....
.....
.....
.....

4.1 How can the encountered challenges be addressed?

.....
.....
.....
.....
.....

ANNEXURE C: INTERVIEW SCHEDULE OF DIRECTORATE FOR PRIORITY CRIME INVESTGATION

1. What is role of Intelligence-Led Policing in the investigation of cybercrime?

.....
.....
.....
.....
.....
.....

2. Which investigative skills are required for one to investigate cybercrime effectively?

.....
.....
.....
.....
.....
.....

3. What are the challenges encountered in the investigation of cybercrime?

.....
.....
.....
.....
.....
.....

3.1 What is the impact of those challenges in successful investigation?

.....
.....
.....
.....
.....
.....

3.2 How can such challenges be addressed?

.....
.....
.....
.....
.....
.....

4. Does the Directorate for Priority Crime Investigation have a focused strategy that deals with cybercrime investigation?

.....
.....
.....
.....
.....
.....

4.1 If the answer to the above question is yes, how effective is such strategy?

.....
.....
.....
.....
.....
.....

5. What is the value of using Intelligence-Led Policing to investigate cybercrime in South Africa?

.....
.....
.....
.....
.....
.....

ANNEXURE D: ETHICAL CLEARANCE



UNISA 2021 ETHICS REVIEW COMMITTEE

Date: 2021:10:25

ERC Reference No.: ST76
Name: PM Matsaung

Dear Mr Pieter Mantjie Matsaung

**Decision: Ethics Approval from
2021:10:25 to 2024:10:25**

Researcher: Mr Pieter Mantjie Matsaung

Supervisor: Prof D1 Masiloane

An exploration of the use of intelligence-led policing in combating cybercrimes in South Africa

Qualification: PhD in Criminal Justice

Thank you for the application for research ethics clearance by the Unisa 2021 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 25 October 2021 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.**
- 2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.**



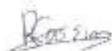
University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 302, UNISA, 2003 South Africa
Telephone: +27 (0) 21 959 3111, Facsimile: +27 12 629 4150
www.unisa.ac.za

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 **2024:10:25**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number *ST/0-2021* should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,



Prof R Cassim
Chair of CLAW ERC
E-mail: cassim@unisa.ac.za
Tel: (012) 429-6780

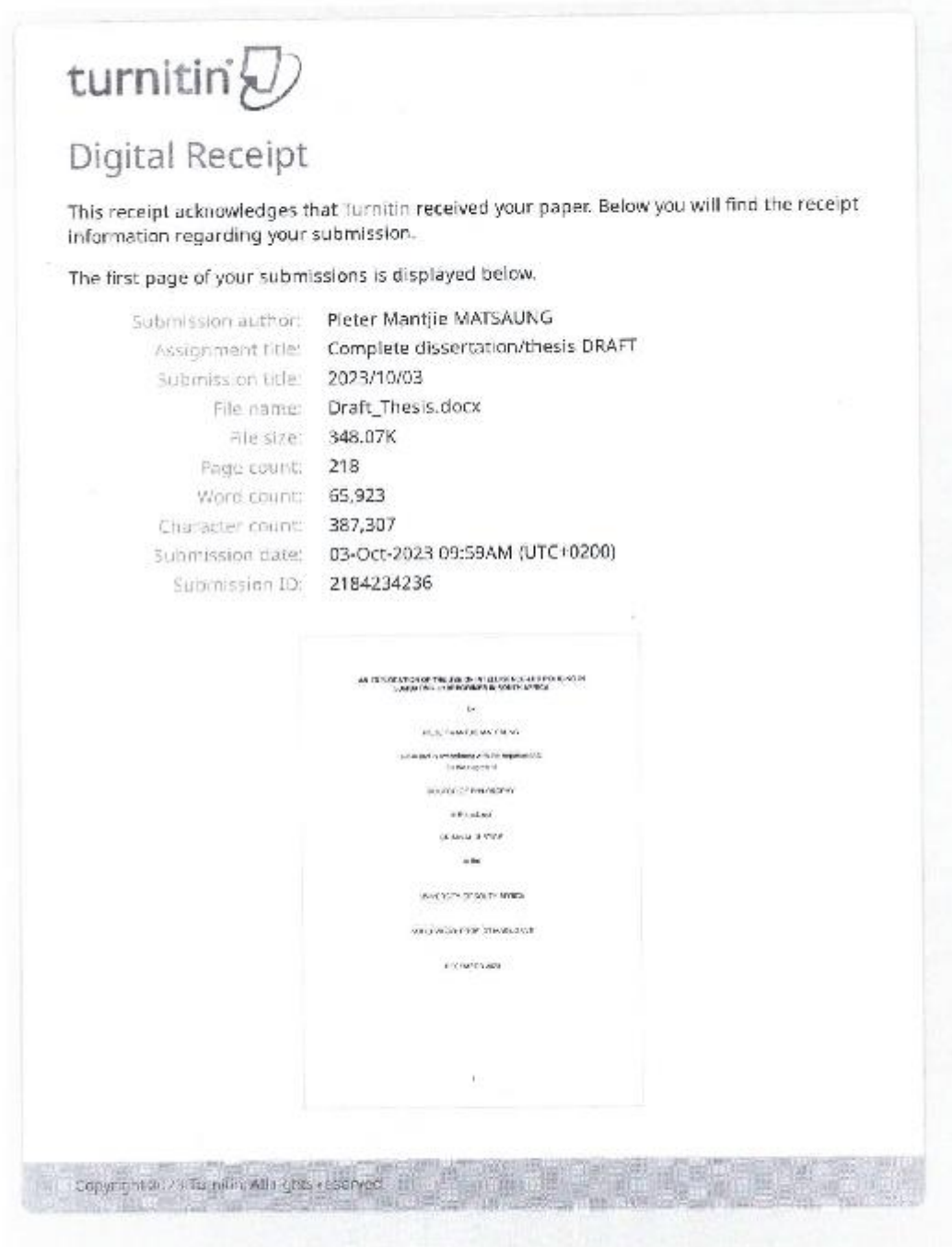


Prof OJ Kole
Acting Executive Dean: CLAW
E-mail: koleo@unisa.ac.za
Tel: (012) 429-8305



University of South Africa
Pretorius Street, Midrand, Johannesburg, City of Tshwane
PO Box 1961 UNISA, DRC3 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE E: TURN-IT-IN CERTIFICATE



The image shows a Turnitin Digital Receipt. At the top left is the Turnitin logo. Below it is the title "Digital Receipt". A paragraph states: "This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission." Another paragraph says: "The first page of your submissions is displayed below." A list of submission details follows, including author name, assignment title, submission title, file name, file size, page count, word count, character count, submission date, and submission ID. Below this list is a small thumbnail of the first page of the document, which is a title page for a dissertation. The title page text is mostly illegible but includes "AN INVESTIGATION OF THE...", "BY...", "SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF...", "SCHOOL OF...", "UNIVERSITY OF...", "2023", and "BY...". At the bottom of the receipt, there is a footer: "Copyright © 2023 Turnitin. All rights reserved."

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: Pieter Mantjie MATSAUNG
Assignment title: Complete dissertation/thesis DRAFT
Submission title: 2023/10/03
File name: Draft_Thesis.docx
File size: 348.07K
Page count: 218
Word count: 65,923
Character count: 387,307
Submission date: 03-Oct-2023 09:59AM (UTC+0200)
Submission ID: 2184234236

AN INVESTIGATION OF THE...
BY...
SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF...
SCHOOL OF...
UNIVERSITY OF...
2023
BY...

Copyright © 2023 Turnitin. All rights reserved.

ANNEXURE F: EDITING CERTIFICATE



Cell: 082 2025 187 | Email: maryna.roodt@gmail.com

EDITOR'S DECLARATION

04-Feb-2021

To whom it may concern:

I, Maryna Roodt, an independent freelance language practitioner, hereby declare that I was tasked to carry out the language editing of the following dissertation:

AN EXPLORATION OF THE USE OF INTELLIGENCE-LED POLICING IN COMBATING CYBERCRIMES IN SOUTH AFRICA

Written by: PIETER MANTJIE MATSAUNG
Student name:
Student number: 4083-327-5

which is submitted in accordance with the requirements for the degree of:
DOCTOR OF PHILOSOPHY in the subject CRIMINAL JUSTICE

After my initial editing, several updates of the entire document were carried out by means of a "question and answer" exercise to render the work as error-free as possible. Please note that I take no responsibility for any alterations and/or errors that were introduced to the document after I finally returned it to the author.

I have extensive experience in copy- editing and have the following qualifications:
BA (major in English); Hons (BA) (English); MA(Applied Linguistics)
and MA (Higher Education Studies).


MP Roodt
maryna.roodt@gmail.com
082 202 5167


Best
The Goodest
Language Nurturer



ANNEXURE G: PERMISSION FROM THE SOUTH AFRICAN POLICE SERVICE

SUID-AFRIKAANSE POLISIEDIENS  SOUTH AFRICAN POLICE SERVICE

Privaatsak/Private Bag X 94

Verwysing/Reference:	3/34/2
Navrae/Enquiries:	Lt Col (Dr) Smit AC Thenga
Telefoon/Telephone:	(012) 393 4333 082 778 8629
Email Address:	ThengaS@saps.gov.za

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

- A. The National Head
DIRECTORATE FOR PRIORITY CRIME INVESTIGATION
- B. The Divisional Commissioner
CRIME INTELLIGENCE
- C. The Divisional Commissioner
DETECTIVE AND FORENSIC SERVICES
- D. The Provincial Commissioners
**FREE STATE
GAUTENG
LIMPOPO
MPUMALANGA
NORTH WEST**

PERMISSION TO CONDUCT RESEARCH IN SAPS: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: AN EXPLORATION OF THE USE OF INTELLIGENCE LED-POLICING IN COMBATING CYBERCRIMES IN SOUTH AFRICA: RESEARCHER: PM MATSAUNG

- A-D. 1. Regarding the abovementioned heading refers.
- 2. The researcher, PM Matsaung, is conducting a study topic/titled: "*An exploration of the use of Intelligence Led-Policing in Combating Cybercrimes in South Africa*" and requests permission to conduct research in the South African Police Services (SAPS).



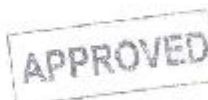
Privatebag Private Bag X94	Pretoria 0081	Faks No. Fax No.	(012) 303 4335
-------------------------------	------------------	---------------------	----------------

Your reference/My verwysing:

My reference/My verwysing: 304/2

THE HEAD, RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0081

Enclosure/Navres: Lt Col (Dr) Smit
AC Thenga
Tel: (012) 393 4333
Email: ThengaS@saps.gov.za



PM Matsaung
UNIVERSITY OF SOUTH AFRICA

**RE: PERMISSION TO CONDUCT RESEARCH IN THE SOUTH AFRICAN POLICE SERVICE:
UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: AN EXPLORATION OF THE
USE OF INTELLIGENCE LED-POLICING IN COMBATING CYBERCRIMES IN SOUTH
AFRICA: RESEARCHER: PM MATSAUNG**

1. The above subject matter refers.
2. You are hereby granted approval for your research study on the above-mentioned topic in terms of National Instruction 4 of 2022.
3. Further arrangements regarding the research study may be made with the following office:

The National Head, Directorate for Priority Crime Investigation:

- **Contact Person:** Brigadier RM Matthews
- **Contact Details:** (012) 846 4325/082 563 5762
- **Email Address:** MatthewsR@saps.gov.za

The Provincial Commissioner: Free State:

- **Contact Person:** Lt Col J Nair
- **Contact Details:** (051) 507 7030/ 082 953 9194
- **Email Address:** NairJ@saps.gov.za

The Provincial Commissioner: Gauteng:

- **Contact Person:** Colonel Govender
- **Contact Details:** (011) 547 9129
- **Email address:** GovenderDN@saps.gov.za
- **Contact Person:** Captain Nevumbani
- **Contact Details:** (011) 547 9189
- **Email Address:** nevumbanivi@saps.gov.za

PERMISSION TO CONDUCT RESEARCH IN SAPS: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: AN EXPLORATION OF THE USE OF INTELLIGENCE LED-POLICING IN COMBATING CYBERCRIMES IN SOUTH AFRICA: RESEARCHER: PM MATSAUNG

3. The research proposal was perused by the Component: Research according to the National Instruction 4 of 2022. Therefore, this office recommends that the research study be permitted, subject to the final comments and further arrangements by the office of the National Head: Directorate for Priority Crime Investigation, the Divisional Commissioners: Crime Intelligence and Detective and Forensic Services as well as Provincial Commissioners: Free State, Gauteng, Limpopo, Mpumalanga and North West.
4. The aim of the study is *"to explore the use of Intelligence Led-Policing in Combating Cybercrime in South Africa"*. Furthermore, the researcher selected to conduct a qualitative research study to collect data from participants by conducting interviews.
5. The researcher, PM Matsaung, intends to collect data by approaching participants who specifically deal with Cybercrime. Therefore, the researcher requested to conduct interviews with seven (7) participants from Crime Intelligence, seven (7) participants from Detective and Forensic Services and seven (7) participants from Directorate for Priority Crime Investigation at Free State, Gauteng, Limpopo, Mpumalanga and North West Province in line with the proposed topic/title.
6. This office hereby requests your support on the condition that your office agrees with our recommendations and confirms the proposed official research is viable. Additionally, your office has the authority to set terms and conditions for the researcher to comply with set standards to be followed during the research study process and not harm the SAPS' image.
7. Kindly find the relevant documents of the requested application topic/titled: *"An exploration of the use of intelligence Led-Policing in Combating cybercrimes in South Africa"* for your consideration:

Annexure A: Application to conduct research;

Annexure B: Signed undertaking;

Annexure C: Research proposal; and

Annexure D: Research approval from the University of South Africa.

**PERMISSION TO CONDUCT RESEARCH IN THE SOUTH AFRICAN POLICE SERVICE:
UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: AN EXPLORATION OF THE
USE OF INTELLIGENCE LED-POLICING IN COMBATING CYBERCRIMES IN SOUTH
AFRICA: RESEARCHER: PM MATSAUNG**

The Provincial Commissioner: Limpopo:

- **Contact Person:** Brig Mphahlele Ngoveni
- **Contact Details:** (015) 290 6250/6097
-
- **Contact Person:** Col B Tau
- **Contact Details:** 015 290 6090/071 602 0396
- **Email Address:** TauBetty@saps.gov.za

APPROVED

The Provincial Commissioner: Mpumalanga:

- **Contact Person:** Col ST Mnisi
- **Contact Details:** (013) 762 4536/079 692 0670
- **Email Address:** MnisiST@saps.gov.za

The Provincial Commissioner: North West:

- **Contact Person:** Colonel TF Goitsilwe
- **Contact Details:** 073 703 7891
- **Email Address:** GoitsilweT@saps.gov.za

- **Contact Person:** Colonel Z Botha
- **Contact Details:** 082 416 0945
- **Email Address:** bothazmi@saps.gov.za

4. Kindly adhere to paragraph 8 of our attached letter signed on 2022-10-03 with the same abovementioned reference number.


MAJOR GENERAL
THE HEAD: RESEARCH
DR PR VUMA

Date: 2022-11-18

PERMISSION TO CONDUCT RESEARCH IN SAPS: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: AN EXPLORATION OF THE USE OF INTELLIGENCE LED-POLICING IN COMBATING CYBERCRIMES IN SOUTH AFRICA: RESEARCHER: PM MATSAUNG

8. The researcher will conduct the research at his/her own expense.
- 8.1 The researcher will conduct the research without disrupting the duties of the participating members of the Service. **In addition, the researcher must communicate and make prior arrangements with the respective commanders of the participating members of the study.**
- 8.2 The researcher, PM Matsaung, should bear in mind that participation in the interviews must be voluntary.
- 8.3 Information will at all times be treated as strictly confidential.
- 8.4 The researcher, PM Matsaung, will provide an electronic copy of the final report to the Service.
- 8.5 The researcher, PM Matsaung, will ensure that the research report complies with all conditions for the approval of the research.
9. Should your office be in agreement with this research request and to facilitate smooth coordination between your office and the researcher, the following information is kindly requested to be forwarded to our office within **18 days** after receipt of this letter.
 - **Signed Certificate/Letter:** Confirm the proposed research request is viable;
 - **Contact person:** Rank, Initials and Surname; and
 - **Contact details:** Telephone number and email address.
10. Your cooperation will be highly appreciated.



THE HEAD: RESEARCH
DR PR VUMA

MAJOR GENERAL

DATE: 2022-10-03

ANNEXURE H: PERMISSION FROM THE DIRECTORATE FOR PRIORITY CRIME INVESTIGATION

Ref no: 3/34/2(50)

INFORMATION NOTE

To: National Head
Directorate for Priority Crime Investigation

APPLICATION TO CONDUCT RESEARCH WITHIN DIRECTORATE FOR PRIORITY CRIME INVESTIGATION: AN EXPLORATION OF THE USE OF INTELLIGENCE LED-POLICING IN COMBATING CYBERCRIMES IN SOUTH AFRICA: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: RESEARCHER: PM MATSAUNG

1. Purpose

1.1. The purpose of the information note is to seek the approval of the National Head for research to be conducted by Researcher: PM Matsaung within the Directorate for Priority Crime Investigation (DPCI).

2. Background

- 2.1. The Researcher: PM Matsaung is conducting a study titled: "An exploration of the use of Intelligence Led-Policing in combating Cybercrimes in South Africa".
- 2.2. The researcher is requesting permission to interview seven (7) members from the Cyber Crime Investigation Section, Priority Crime Specialised Investigation, Directorate for Priority Crime Investigation (DPCI).

3. Attachments

- 3.1. Application letter from Division: Research with ref. number 3/34/2 dated 2022-10-03
- 3.2. Research proposal (Detail of studies) which contains the following:
- Problem Statement
 - Research Objectives
 - Research questions
- 3.3. The research application has been perused and recommended for permission by the Division: Research and found to be compliant with the National Instruction 1 of 2006: Research in the South African Police Service.

APPLICATION TO CONDUCT RESEARCH WITHIN DIRECTORATE FOR PRIORITY CRIME INVESTIGATION: AN EXPLORATION OF THE USE OF INTELLIGENCE LED-POLICING IN COMBATING CYBERCRIMES IN SOUTH AFRICA: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: RESEARCHER: PM MATSAUNG


BRIGADIER
SECTION HEAD: STRATEGIC MANAGEMENT
DIRECTORATE FOR PRIORITY CRIME INVESTIGATION
RM MATTHEWS

Date: 2022-10-05

Application recommended/ not recommended


Comments: Copy of the completed user research study
must be submitted to DPCI upon completion


MAJOR GENERAL
COMPONENT HEAD: GOVERNANCE AND CORPORATE SERVICES
DIRECTORATE FOR PRIORITY CRIME INVESTIGATION
DM MOLATJANA

Date: 2022/10/06

Application recommended/ ~~not~~ recommended

Comments:


LIEUTENANT GENERAL
ACTING DEPUTY NATIONAL HEAD: DIRECTORATE FOR PRIORITY CRIME INVESTIGATION
(ADV/CFE) SC MOSIPI

Date: 2022-10-08

APPLICATION TO CONDUCT RESEARCH WITHIN DIRECTORATE FOR PRIORITY CRIME INVESTIGATION: AN EXPLORATION OF THE USE OF INTELLIGENCE LED-POLICING IN COMBATING CYBERCRIMES IN SOUTH AFRICA: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: RESEARCHER: PM MATSAUNG

Application approved/ ~~not approved~~ ✓

Comments:


LIEUTENANT GENERAL
NATIONAL HEAD: DIRECTORATE FOR PRIORITY CRIME INVESTIGATION
(DR/ADV) SG LEBEYA (SOEG)

Date: 2022-10-10

Information note compiled by : Brigadier RM Matthews
Telephone number : 082 569 5762
Date : 2022-10-05

Information note perused by : Major General Molatjana
Telephone number : 072 730 8158
Date : 2022-10-05