An Exploratory Study of the South African Police Services (SAPS) Systems in Combating Cybercrimes.

By

Slindile Ngcece

Student Number: 214519385

Submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

Criminology and Forensic Studies

School of Applied Human Sciences

at the

University of KwaZulu-Natal (Howard College)

South Africa

Supervisor: Dr Sazelo Mkhize

2025

DECLARATION

I hereby declare that the thesis, "An Exploratory Study of the South African Police Services (SAPS) Systems in Combating Cybercrime," represents my work both in conception and execution. It has never been submitted nor published for the award of any degree. All the sources consulted or quoted have been cited and acknowledged utilizing in-text and end-text referencing

[redacted] 05/04/2025

Candidate's Signature **Date**

DEDICATION

This thesis is dedicated to my late Grandmother, **Grace Rebecca Ngcece,** and my late aunt, **Busisiwe Hadebe**. How I wish you were here to witness my achievement. Your teachings, values, and the importance of education you instilled in me, I kept holding on to them.

To my two sons, **Phiwokuhle and Gcinokuhle**, I had both of you during the most critical years of my PhD journey, and juggling motherhood and studying was not easy. Having you, however, inspired me to work harder, not only for myself but also for you, my children, and your future.

ACKNOWLEDGMENT

First and foremost, I want to express my gratitude to God, the Almighty, and the Creator for providing me with the strength and determination to overcome all the challenges I encountered during this phase and enabling me to complete this research project.

Secondly, I am indebted to many people who, in diverse ways, played various roles to assist me during my PhD journey. Without them, this study would not have seen the light of day. Unfortunately, space constraints do not make it possible to mention all of them. However, it is fair to particularly acknowledge a select few; and in that regard:

- My sincere gratitude goes out to Dr. S. Mkhize, my supervisor, for his support, inspiration, guidance, and constructive criticism, and, most importantly, for having faith in my abilities.
- I would also like to thank the National Research Foundation (NRF) for funding this project. I am forever grateful.
- To the South African Police Services (SAPS) police officers who gave their time and energy, showed support, shared their knowledge, and contributed to the study's success, I thank you.
- To the Ngcece family, who gave their staunch support, I am grateful.
- To my loving friends whom I consider my sisters, Nonhle Sibisi, Phumelele Magwaza, and Thembeka Madinane, Thank you so much for all the support, encouragement, and prayers throughout my PhD journey. I appreciate your goodwill.

ABSTRACT

The rapid development of technology and computing has tremendously changed people's lives and how crime is committed in modern societies. The digital revolution and increase in internet connectivity have created not only new opportunities for wealth creation but also the potential for transactional offending, posing a major threat to governments, business organizations, and individuals. Globally, cybercrime leads to financial losses, reputational damage, and personal information data breaches. South Africa is not an exception. In 2018, the country was ranked amongst the top ten countries on the cybercrime predator list, making the country appear to be a major attraction to cybercriminals. The country is estimated to lose about R2.2 billion a year to cyber-attacks. Although there is an increase in research output on cybercrimes, some areas of the phenomenon are least explored, particularly how law enforcement agencies in South Africa respond to the challenges associated with online crimes. The study, therefore, explores how the South African Police Services (SAPS) responds to cybercrimes and offer practical solutions. It seeks to identify the types of cybercrimes, challenges that SAPS has encountered, and measures taken to combat them. The study also aims to determine if any intervention strategies need to be reviewed and/or if new approaches must be developed to deal with cybercrime effectively. Conducted in Durban, KwaZulu Natal, the study adopted the phenomenological research design, according to which interpretive and constructivist qualitative research paradigms were deemed appropriate. They allow participants to describe their understanding, interpretations, and personal experiences of cybercrimes in South Africa. Data was collected through in-depth interviews using semi- structured interviews, with a sample of 17 participants purposively drawn from the Directorate for Priority Crime Investigation (DPCI) and the Commercial Crimes Unit (CCI) of the South African Police Service (SAPS). The theoretical orientations that guided the study are the Routine Activities Theory and the Structural Functionalism Theory. The study revealed that South Africa has been experiencing a variety of cybercrimes, including cyber fraud, identity theft, and phishing attacks, and most of them were perpetuated for financial gain. The study also found that South Africa has introduced laws and security strategies, such as the Cybercrime and Cybersecurity Bill of 2017, to respond to cybercrimes. The challenge, however, is that these laws and legislation are not adapting fast enough to deal with the constantly changing technological environment and the new emerging types and methods of cybercrimes. Police officers who are experts in the field and can respond to cybercrimes are limited. They also do not have enough resources and require constant training to keep up to date with

technological advancements and criminal activities. Above all, it has become increasingly evident that there is a need for the collaboration of all stakeholders, including prosecutors and the judiciary, private security agencies and investigators, electronic communication service providers (CSPs), and/or Internet service providers (ISPs) if cybercrimes are to be tackled effectively.

Keywords: *Cybercrimes, South African Police Service, Cybercriminals, Cybersecurity, Policies, Law enforcement, Technology, Internet.*

LIST OF ABBREVIATIONS

IT	Information Technology
SAPS	South African Police services
ECSP	Electronic Communications Service Providers
SA	South Africa
CPA	Criminal Procedure Act
ECT	Electronic Communications and Transactions Act
RICA	Regulation of Interception of Communications Act
POCA	Prevention of Organized Crime Act
FICA	Financial Intelligence Centre Act
POPIA	Protection of Personal Information Act
NCFP	National Cybersecurity Policy Framework
ICT	Information Communication Technology
ISP	Internet Service Provider
AU	African Union
NPF	Nigerian Police Force
EFCC	Economic and Financial Crimes Commission
GPS	Global Positioning System
GIS	Global Information System
KICA	Kenya Information and Communications Act
KDPA	Kenyan Data Protection Act
LSK	Law Society of Kenya
CCRC	Cybercrime and Computer-Related Crimes Act
MCERT	Malawi Computer Emergency Response Team
ECOWAS	Economic Community of West African States
CECC	Council of European Convention on Cybercrime
UK	United Kingdom

CFAA	Computer Fraud and Abuse Act
NIIPA	National Information Infrastructure Protection Act of 1996 (
ECPA	Electronic Communication Privacy Act
COPPA	Children's Online Privacy Protection Act
CANSPAM	Controlling the Assault of NonSolicited Pornography and Marketing Act
EITL	Electronic Information and Transaction Law
NIST	National Institutes of Standards and Technology
DSL	Data Security Law
PDA	Personal Digital Assistant
AI	Artificial intelligence
ML	Machine Learning
UNECA	UN Economic Commission for Africa
CLOUD	Clarifying Lawful Overseas Use of Data Act
SARS	Special Anti-Robbery Squad
CSO	Civil Society Organizations
MSSCA	Multi-Split Spam Corpus Algorithm
IM	Instant Messaging
DoS	Denial of Service Attacks
ENISA	European Network and Information Security Agency
CID	Cyber Intelligence Division
BDA	Blockchain-based digital assets
KZN	KwaZulu Natal
DPCI	Directorate for Priority Crime Investigation
HSSREC	Humanities and Social Sciences Research Ethics Committee
FBI	Federal Bureau of Investigation
RAT	Routine Activities Theory

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

APPENDICES

CHAPTER ONE

INTRODUCTION

1.1 Introduction and Background of the Study

In the past few decades, the exponential growth of internet connectivity has offered humanity enormous socio-economic benefits and fundamentally altered the way people live, work, and relate to one another. However, the enormous benefits of internet connectivity have not only spawned global e-commerce, digital payments, digital transformation initiatives, internet and mobile usage, cloud computing adoption, and an increase in output and wealth generation. There also remain high risks associated with interconnectivity, with the dynamic development of cybercrime threatening to corrode the gains of the digital revolution (Kuzior, Tiutiunyk, Zielińska, & Kelemen, 2024). Kuzior et al. (2024) state that as the world becomes increasingly digital, with more online transactions and activities, the risk and impact of cybercrime grow. Citing a report from the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center, cybercrime resulted in $10.3 billion in losses in 2022, up from $6.9 billion in 2021. According to IBM's report (2024; cited in Kuzior et al., 2024), the average cost of a data breach worldwide increased to USD 4.45 million in 2023, up by USD 100,000 from 2022, which marks a 2.3% rise from the 2022 average cost of USD 4.35 million.

Since 2020, when the average total cost was USD 3.86 million, the overall average price and data breaches have risen by 15.3% worldwide, and the most significant contributory factor is the outbreak of the COVID-19 pandemic (IBM, 2024). The COVID-19 outbreak did not only spawn even greater internet connectivity and a rise in remote working (Khan, Saleh, Dorasamy, Khan, Leng &sw Vergara, 2023). It also contributed to the increase in cybercrimes, leading to "significant financial loss as businesses suffer from operational disruptions, reputational damage, and direct financial theft" (Kuzior et al., 2024:222). The challenges of cybercrime are, however, not limited to businesses and individuals; governments also fall victim, where cybercrime, respectively, involves the theft of sensitive personal data or information stored online and cyber-attacks on critical infrastructure (for example, power grids and healthcare systems). In both instances, the individual's reputation, privacy, and national security could be compromised.

Kuzior et al. (2024) point out (citing Verizon Business, 2023) that with 83% of data breaches involving sensitive personal information, there is a critical need for robust data protection measures to safeguard privacy and maintain trust among users and customers. This has been a global trend, and the measures include various national, regional, and international cyber instruments.

At the international and regional levels, the cyber instruments to combat cross-border cybercrimes include:

- A Draft United Nations Convention on Cooperation in Combating Cybercrime, proposed by Russia in 2017 (A/C.3/72/12)
- The Council of Europe's Convention on Cybercrime of 2001
- The Commonwealth of Independent States' Agreement on Cooperation in Combating Offences related to Computer Information 2001.
- Arab Convention on Combating Information Technology Offences of 2010.
- The Shanghai Cooperation Organization's Agreement on Cooperation in the Field of International Information Security of 2010.
- African Union Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa (Draft African Union Convention) of 2012.
- African Union Convention on Cyber Security and Personal Data Protection of 2014
- Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime of 2012.
- The Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime of 2011. This directive requires member states to criminalize cybercrime in national law and facilitate mutual legal assistance, cooperation, and extradition in cybercrime and cybersecurity-related matters. ECOWAS has a Convention on Mutual Assistance in Criminal Matters and a Convention on Extradition to facilitate cooperation in cybercrime investigations and extradite cybercriminals (UNODC, Online).

At the national level, various legal and administrative frameworks for cybersecurity have also been developed to complement international cyber instruments in the fight against cybercrimes. In Mauritius, for example, the Computer Misuse and Cybercrime Act was enacted in 2003. In

Kenya, the Computer and Cyber Crimes Act of 2018 is still the cornerstone of that country's cybersecurity legislative framework, and in Ghana, the Cybersecurity Act of 2020 and the Ghana National Cyber Security Policy & Strategy of 2014 have been the core national cyber instruments to combat cybercrime.

Despite all the national and international cybersecurity interventions, cybercrime is rising exponentially. Cybersecurity statistics show that Africa is the worst-off region, with only 30% of the countries having a Global Cybersecurity Index (GCI) of 50.0 or more as of 2021, compared with the rest of the world (ITU, 2021). At the top of the list was Mauritius, with a GCI of 96.89, followed by Egypt (95.48), Tanzania (90.58) and Ghana (86.69). South Africa was ranked 11th, with a GCI of 78,46 (Table 1), indicating a relatively worsening state of cybersecurity. In some respects, South Africa appears to be the hardest hit compared with some African countries with similar levels of development. It has been acknowledged as one of the most cyber-attacked developing countries (Mapimele & Mangoale, 2019).

Table 1.1 Top 15 Countries in Africa Regional Ranking GCI 2020*

Country Name	Overall Score	Regional Rank	Global Rank
Mauritius	96.89	1	17
Egypt	95.48	2	23
Tanzania	90.58	3	37
Ghana	86.69	4	43
Tunisia	86.63	5	45
Nigeria	84.76	6	47
Morocco	82.41	7	50
Kenya	81.7	8	51
Benin	80.06	9	56
Rwanda	79.95	10	57
South Africa*	78.46	11	59
Uganda	69.98	12	72
Zambia	68.88	13	73
Côte d'Ivoire	67.82	14	75
Botswana	53.06	15	88

Source: ITU, 2021

* No response to the questionnaire/data collected by the GCI Team

South Africa is estimated to have lost US$242 million in 2016, the estimates also show that the country loses US$157 million annually to cybercrime. Furthermore, 67% of South African residents claim to have encountered some form of online crime compared to 48% of people globally. An estimated 20% of South Africans are sharing confidential information (such as passwords) with others through social network platforms, while 21% claim to engage with strangers online (Mabaso, 2018 & Maluleke, 2023). This raises questions about the public's knowledge of cybersecurity dangers, the capacity of the police, and, for that matter, the government to protect its citizens and the country's cyberspace. It also raises questions about the effectiveness of the legislative framework in maintaining the country's cybersecurity and safety. Several cybercrime strategies have been created in South Africa to fight against cybercrime and secure the use of information and communication technologies. The Cybercrimes Bill is South Africa's first legislative response to cybercrime, following the Electronic Communication and Transactions Act (ECTA) enacted in 2002. Among others is a National Cyber Security Policy Framework (NCPF), approved in September 2015 (Mabunda, 2021).

Although the government has recognized the need for cyberspace security to protect the country and its citizens, Mabaso (2018) argues that South Africa is still unable to implement clear and adequate cybersecurity strategies systematically. The biggest impediments are the slow pace at which the NCPF is being implemented and the inadequacy of resources and capacity. Besides the overarching challenges of violent crimes in South Africa, cyberspace security does not appear to be a number one priority for the government. Cybercriminals do not only find innovative ways but also use the anonymity of communication technologies, such as Telegram and Tor, to evade arrest and prosecution. Although South Africa's response to cybercrime has mostly been reactionary, it is fair to argue that the dark web compounds the problem by using a technology known as "onion routing" to protect internet users – including, ironically, cybercriminals - from surveillance and tracking. Onion routing is an anonymous internet network that makes it hard to track down a user's location or activity by passing information through several encrypted "onion" layers (Nastula, 2019). Cybercriminals utilize anonymous communication devices (such as The Onion Router) for example, to open-source e-commerce protocol that uses cryptocurrency to hide illegal transactions (Nastula, 2019)

Indeed, in 2018, the country was ranked among the top ten countries in Africa with regard to cyber-attacks (Mabaso, 2018) and has since not had a safe space from cyber threats. Recent cyberattacks have exposed its vulnerability to cyber criminals and ransomware attacks (Olofinbiyi, 2022). To identify and anticipate new types of cybercrime, one must have the capacity not only to respond proactively but also to enjoy the support and cooperation of key stakeholders, including web owners (Mapimele & Mangoale, 2019). Moreover, for South Africa to adequately deal with cybercrime, more research and comprehensive understanding are essential within the government to create focused laws and policies to effectively deal with cybercrimes and their negative impacts (Mtuze, 2022).

1.2 Research Problem

Cybercrime is an unprecedented, fast-growing threat in and between countries (Khan, Saleh, Dorasamy, Khan, Leng, & Vergara, 2023). Many countries increasingly rely on cyberspace and digital devices to conduct business, day-to-day activities, and governance (Mabaso, 2018). This, therefore, increases the opportunity for and the scale of cyberattacks. Many organizations in both private and public sectors have experienced substantial financial losses due to cybercrimes. According to the South African Banking Risk Information Centre (SABRIC), South Africa currently has the third-highest number of cybercrime victims worldwide, with the country losing an estimated R2.2 billion a year to cyber-attacks (Gumbi, 2018). The issue of cybercrime is escalating, and it is uncertain if law enforcement agencies have the capacity and ability to adequately investigate and prosecute online offenders (Mugisha, 2019).

Collier, Thomas, Clayton, Hutchings, and Chua (2022) state that these phenomena (cybercrimes) often appear random and unpredictable, making them difficult for local law enforcement to tackle. Further, online crimes create issues for standard police strategies, such as jurisdictional issues and anonymity technologies. This is because they (online crimes) differ from traditional crimes in terms of their operational context, symbolized by their peculiar technical platforms, infrastructure, and social spaces. These pose a challenge to the criminal justice system's personnel, many of whom are struggling to grasp the fundamental aspects of technology-aided crimes. Police officers need to fully understand the illicit use of technology to impact conviction rates. Mugisha (2019) argues that although, at some level, issues of digital investigations are being addressed, the majority of the

police force still lacks an understanding of the potential value of digital evidence, inversely leading to a lack of resources to address it. Furthermore, a study by Mugisha (2019) indicates that only a limited percentage of law enforcement officials had basic skills in computer forensics and found it difficult to respond to incidents of cybercrimes. Despite the prevalence of technology, state and local law enforcement agencies lack the training, tools, and adequate personnel to effectively conduct investigations, throwing them under the spotlight regarding their capacity and competency in dealing with the increasing rate of cybercrime.

Based on these observations, it is fair to argue that since the use of digital devices has increased, so has been an increase in the variety of digital devices with complicated settings and digital processors or storage media. This, evidently, calls for a continuous need for new tools, approaches, and strategies to deal with digital forensic investigations. According to Awoyemi, Omotayo, and Mpapalika (2021), cybercrime also poses a danger at national and cross-border levels, extending beyond state and regional boundaries. Cyberspace has expanded due to modern information and communication technology, putting nations in danger. Moreover, Cybercriminals take advantage of weak border controls and inadequate law enforcement to extend their operations internationally. They frequently launder money in nations with less strict regulations and operate undetected in corrupt and inefficient regulatory environments (Awoyemi, Omotayo, & Mpapalika, 2021). According to Dlamini and Mbambo (2019), another challenge in policing cybercrime is the gap between the process by which the systems and policies are implemented and the advancement of technology. Cybersecurity systems and policy development progress slowly, especially in African countries.

According to Muller (2015), South Africa lacks clearly defined cybercrime strategic defenses and coordinated approaches to deal with cybercrime. The current approaches do not deal holistically with the challenges of cybercrime. This is, however, not peculiar to South Africa. Many developing countries have been unable to build the infrastructure needed to secure systems in cyberspace. Although developing countries may receive assistance in building security structures, they still cannot sustain these mechanisms in the long term. The failure to build and maintain systems results in dependency or reliance on other countries (Muller, 2015). The scarcity of proper networks, infrastructure, and security and an unclear legal framework means greater risks and higher chances of being targeted by cybercriminals.

Policymakers need to close the gap between the creation and execution of policies as soon as possible. Inadequate stakeholder training and out-of-date policies impede effective enforcement, and government agencies often neglect to take active roles in cybercrime concerns. In this regard, collaboration between academics, business, government, and other stakeholders is increasing, but more has to be done, particularly cooperation between the private and public sectors (Dlamini & Mbambo, 2019). It has also been observed that most of what constitutes "the internet" is owned by private technology companies, who apparently have more knowledge of cyberspace security (Muller, 2015). However, cooperation between the private and public sectors is still challenging. This results in the public sector being unable to access the same level of knowledge and information as the private sector to secure cyberspace. Effective cooperation between the two sectors would empower the key players in the public sector and effectively contribute to combatting cybercrime holistically.

Much of the literature, including Baylon and Antwi-Boasiako (2017) and Kshetri (2019), concur that inadequate financial and human resources are one of the challenges facing law enforcement agencies in combating cybercrime. Baylon and Antwi-Boasiako (2017), for instance, maintain that insufficient funding is not only a major constraint in the training of police officers but also the acquisition of appropriate equipment to conduct digital forensics. Kshetri (2019) also argues that law enforcement agencies lack manpower, technical skills, and knowledge to deal with cybercrimes. Many police officers are often not adequately equipped with the necessary technical skills to undertake digital forensics investigations. Moreover, the high rate of labor force turnover deprives law enforcement agencies of the few technically trained police personnel in the public sector, who often tend to leave after acquiring the necessary digital skills to join the private sector (Baylon & Antwi-Boasiako, 2017).

Undoubtedly, there are not only several but also diverse constraints to combatting cybercrime. It was, therefore, imperative to find out how the South African Police Services (SAPS) have dealt with and responded to cybercrimes and whether they have been successful in dealing with cybercrime to help maximize the benefits of cyberspace and cybersecurity. This is the focus of this study.

1.3 Aim of the Study

The study explores how South African Police Services (SAPS) combat cybercrimes. This study seeks to understand the cybercrime combating platforms endorsed by SAPS and how best they have responded to cybercrimes. The study also addresses cyber threats and challenges posed by cyberspaces and cyber-offenders in South Africa. It seeks to examine the legal framework that guides cybersecurity and information systems and determine how best they could be strengthened to prevent cybercrimes effectively.

1.4 Objectives of the Study

The study was designed to meet the following objectives.

I. To identify the systems currently employed by SAPS to curb cybercrimes.

This objective identifies the measures, including strategies and laws, that have been implemented to eliminate, reduce, and/or prevent cybercrimes in South Africa. By identifying the measures, the study will be able to determine whether SAPS is behind, at par with, or ahead of international best practices in combatting cybercrime. It will also help to determine the extent to which the interventions are appropriate regarding the nature and type of cybercrime it is intended to target.

II. To determine the effectiveness of SAPS systems in responding to cybercrimes.

This objective aims to evaluate whether the measures, including policies and strategies employed by law enforcement agencies, are effective in responding to online crimes. Determining the effectiveness of the interventions will help to determine which of the policies, programs, and laws are working or not and pave the way for policy recommendations that can contribute to the elimination, reduction, and/or prevention of cybercrimes in South Africa and, by extension, other African countries and the world in general.

III. To investigate the types of cybercrime that SAPS encounters

Cybercrimes are a global challenge, and South Africa is not immune to it. This objective is to explore the types and nature of cybercrimes committed in South Africa. It also focuses on the frequency of occurrence and the *modus operandi* of cybercriminals.

IV. To identify the challenges that SAPS encounters in dealing with cybercrime.

This objective looks at the challenges, if any, that law enforcement agencies are facing in combating cybercrimes. Technology is advancing, and so is the increase in cybercrime. Criminals are always up to date and even ahead of law enforcement agencies, adapting and being sophisticated in their criminal activities and ways of offending. What impact or influence does this then have on law enforcement and effective response to cybercrimes?

V. To recommend Interventions that SAPS can adopt to curb cybercrime.

This objective explores recommendations that SAPS can adopt to improve cybersecurity and safety in South Africa, focusing on policies, strategies, laws, etc., to fight against cybercriminals.

1.5 Underlying Questions

This research study aimed to address the following research questions in accordance with the study's goals.

I. What systems are currently implemented by SAPS to curb cybercrime?

II. How effective are the existing SAPS systems in dealing with cybercrimes?

III. What types of cybercrimes do SAPS encounter?

IV. What are some challenges SAPS encounters when dealing with cybercrimes?

V. What interventions can be recommended for SAPS to adopt to curb cybercrime effectively in South Africa?

1.6 Significance of the Study

There is a shortage of investigations about the presence of specialized systems used to decrease and respond to cybercrime in South Africa. Du Toit, Hadebe, and Mphatheni 2018; Kshetri, 2019; Mabaso, 2018; and Dlamini and Mbambo (2019) maintain that there is a rise in cybercrime in South Africa. However, there is limited research on the presence of cybercrime-combatting systems in South Africa and whether they have been effective. The public relies on the police to protect and deal with online crimes, which impact negatively on their lives.

Therefore, effective strategies and broad policy guidelines on cyber-security in the country ought to be developed, and such strategies and guidelines ought to be evidence-based. Developing evidence-based measures and strengthening SAPS' combatting cybercrime capacity can contribute towards enhancing and protecting the country's public and private sectors information systems and/or structures, as well as individuals from the trauma of identity theft and financial loss. Thus, through studies of this nature, threats to cyberspace systems can be uncovered, which in turn can encourage the government to become more proactive in combating cybercrime and enable SAPS to initiate strategies that can improve the policing of cybercrimes. The study is of importance to the police or investigators, security agencies, and other stakeholders involved in cybersecurity management because it proposes security measures and network resources that can assist the police in combatting cybercrimes. Moreover, it explores and helps law enforcement agencies to understand factors impeding the investigation and prosecution of cybercrime offending. In that manner, it raises awareness, exposes the barriers to justice, and increases conviction rates. An increase in convictions may mean an increase in the reporting of cybercrimes.

Finally, as Li (2018) argues, victims often suffer in silence, unaware of the laws or systems in place to protect them. The success of this study could assist the public in understanding and raising awareness of the risks associated with cyberspace. Awareness and proper education on cybercrime could instill and promote a positive mindset or behaviours of cyberspace users toward cybersecurity culture. South Africans need to be better informed about the constantly evolving methods used by cybercriminals to victimize them. If law enforcement could take a more proactive stance towards advancing detection and responding techniques to cybercrimes, they could close the gap that cybercriminals exploit at the expense of unsuspecting cyberspace users. Cybercriminals are sophisticated; therefore, it is imperative to increase public awareness of cybercrimes and address cybersecurity management as a matter of urgency.

1.7 Conceptualisation of Terms

Writing precise definitions for our main concepts is necessary in the conceptualization process (Madina, 2023). The concepts used throughout the research study are defined in this section for better understanding and clarification.

1.7.1 Cybercrimes

Du Toit, Hadebe, and Mphatheni (2018) define cybercrime as any crime committed using a computer via the Internet. The computer can be used as a tool or a target to participate in illegal and/or unethical online behavior. While Ismail (2020) refers to cybercrimes as the illegal use of computer technology in cyberspace that impacts computer systems or data. There is no universally accepted definition of cybercrime. It is sometimes used interchangeably with phrases such as computer crime, high-tech crime, cybernetic crime, computer-related crime, or digital crime. In this study, cybercrime is any crime committed against an individual using a computer, technology, or the internet.

1.7.2 Cybersecurity

Cybersecurity is the process of securing networks, devices, and data against illegal or unauthorized access while maintaining data availability, confidentiality, and integrity. Cybersecurity also means protecting and securing confidential data, including usernames, passwords, full names, addresses, etc. (Nnaemeka, 2023). Cybersecurity is especially important in the modern digital age, where communication, entertainment, trade, transportation, and even healthcare depend on computers and the internet. This research defines cybersecurity as the measures implemented by governmental organizations to protect the general public and their operations against cyberspace dangers.

1.7.3 Cyberspace

Cyberspace is a worldwide web that is part of the information environment. It comprises networks of interconnected information technology infrastructures, including computer systems, embedded processors and controllers, telecommunications networks, and the Internet. It is also defined as a three- dimensional virtual environment mostly made up of information and used for computer network communication (Bay, 2016). This research defines cyberspace as a set of information systems and the people who use them to communicate.

1.7.4 Internet/Online

The Internet is an electronic communications network that links global organizational and computer networks. It is a global network of computers, servers, phones, and smart appliances that facilitate quick information transmission and reception. Internet Acting as a hub for

computer networks enables users to communicate and receive data from other systems (Nnaemeka, 2023). The internet infrastructure includes Local and wide area networks, metropolitan area networks, and optical fibre data transmission cables. Wi-Fi and other wireless services like 4G and 5G are part of internet infrastructure.

1.7.5 Cyber laws

Babikian (2023) defines cyberlaw as the legal frameworks and laws that control digital activity. It is often referred to as internet law or digital law. It addresses a wide range of issues, including digital privacy, e-commerce, online communication, and the detection and penalties of cybercrimes. Cyberlaw provides legal protections for people and companies utilizing the internet (Nnaemeka, 2023). Given the growing importance of the internet in our everyday lives, cyber law is essential to maintaining the safe and orderly operation of digital space.

1.7.6 Law enforcement - South African Police Services (SAPS)

Law enforcement describes the organizations and professionals responsible for upholding and enforcing the law, promoting public order, and ensuring safety. Their main responsibilities are to investigate, apprehend, and detain those accused of committing crimes. Police services have always been viewed as a crime prevention force. However, contemporary law enforcement agencies today provide the community with a range of services, including administrative, regulatory, social welfare, and law enforcement (Tomkins, 2005). The SAPS looks at enforcement as a community-oriented service, prioritizing the fundamental rights of all South African people. It involves the community as important stakeholders and operates flexibly and collaboratively. This approach necessitates mechanisms like Community Police Forums and civilian involvement in policing matters.

1.7.7 Cybercriminals/ Cyber offenders

A cybercriminal is a person who uses digital technology, such as computers or the Internet, to commit crimes. They perpetrate crimes like hacking, identity theft, online fraud, and scams. They attack computer systems and employ a variety of tools, technological skills, and a knowledge of human behaviour to victimize individuals and organizations (Sammons & Cross, 2017)

1.8 STRUCTURE OF THE THESIS

This study comprises six chapters. An outline of each chapter is provided below:

Chapter One: Introduction

The chapter presents an introduction and background of the study. It highlights the aim of the study, objectives, and the relevant research questions that the study explored. The study's important concepts were outlined, and the research problems on cybercrimes are stated in this chapter. This chapter also presents the significance of the research and its conclusions

Chapter Two: Literature Review

This chapter presents a review of relevant literature and scholarly investigations on cybercrimes. It critically reviewed previous studies and thus identified the gaps in the literature with specific reference to cybercrimes and the policing of cybercrimes.

Chapter Three: Theoretical Framework

Chapter three provides a theoretical framework that supports the study. Namely, the Structural Functionalism Theory and The Routine Activities Theory (RAT). The researcher viewed these criminological theories as appropriate to guide, describe, and interpret the study and its findings. They informed the criminological analyses of how the police services respond to and/or deal with cybercrimes and challenges within the South African context.

Chapter Four: Research Methodology

This chapter reflects on the research methodology section and provides in-depth information on how the study was conducted. In this chapter, the methods employed for the research study are explored, focusing on research design, Approach, study location, study population and sample size, sampling techniques, data collection, data analysis, ethical considerations, and limitations of the study.

Chapter Five: Presentation of Findings

Chapter five focuses on the analysis, interpretation, and presentation of the data that were collected during the fieldwork or Primary data collection phase of the project. The chapter

addresses the findings that emerged from the identified themes for comparative and reflective purposes.

Chapter Six: Conclusions and Recommendations

The chapter illustrates the overall conclusions of this thesis. It summarizes the main findings, draws relevant conclusions, and offers policy recommendations for combating cybercrimes.

1.9 CONCLUSION

This chapter introduces the main problem of the study and its background. It has indicated the aims and objectives of the study and thus revealed the purpose and relevance of the study. The chapter has indicated and explained the important concepts explored interchangeably throughout the study. Furthermore, the chapter has provided a breakdown of the thesis and a brief indication of what the subsequent chapters encompass. These chapters will be discussed in more detail throughout the thesis.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter examines the literature that focuses on the crucial and particular research areas on cybercrimes. The reviewed academic literature enables the researcher to comprehend the nature and significance of the identified problem more thoroughly. The International and local academic literature on cybercrimes was accessed to find relevant information that answers the topic under study and its objectives. The study's objective is to understand and explore techniques or measures employed by law enforcement, governments, or countries to combat cybercrimes. It seeks to understand the challenges and effectiveness of policing cybercrimes. The types of cybercrimes that police officers often encounter in their work are also discussed.

Much of the literature, including Gumbi (2018) and Mabunda (2021) agrees that internet connectivity in Africa has significantly increased. However, while public and private sectors, as well as individuals, are reaping the benefits of the digital revolution, little attention is paid to cyber security and safety, allowing fraudsters and cybercriminals to take advantage of the growing broadband connectivity to commit cybercrimes at huge costs to the state, corporate bodies, and individuals. The public's lack of information technology (IT) awareness and appropriate legal frameworks to deal with cybercrime at the national and regional levels have exacerbated the cybercrime problem. Developments in cyberspace, however, indicate that considerable efforts are being made in Africa to combat cybercrime. The government of South Africa, for instance, has taken steps to enact cybercrime laws (Gumbi, 2018). However, there are challenges in fighting cybercrime. Some of the difficulties arise from the borderless nature of cybercrimes. For example, collaboration with cross-border authorities tends to be problematic. There are issues of jurisdiction and undue delays in the investigation of cybercrime cases (Wang, Hsieh, Chang, Jiang & Dallier, 2020). There are also issues of protocols that need to be followed with some of them political in nature, which could also delay cases in instances where cross-border suspects have to be extradited for trial and possible conviction.

2.2 Systems Employed to Curb Cybercrimes in South Africa

Mabunda (2021) states that countries have developed cyberspace administrative policies and procedures, laws, and regulations to ensure cyber security and safety. South Africa is not an exception. The South African Police Service (SAPS), like all other law enforcement agents globally, is legislatively mandated to, among other functions, enforce the country's cyberspace legislative instruments. The instruments which are embodied in the National Cyberspace Legislative and Policy Framework include the Cybercrime and Cybersecurity Bill, the Electronic Communications and Transactions Act 25 of 2002 (ECT), the Protection of Personal Information Act (POPIA), and the National Cybersecurity Policy Framework (NCFP). Besides the South African National Cybercrime Legislative and Policy Frameworks, there are also International Cyberspace Conventions and Legislative Frameworks. The list includes the United Nations Conventions on Cybercrime, the United Nations Cyber Security Treaty, the Council of Europe's Convention on Cybercrime (The Budapest Convention), and the African Union (AU) Convention on Cybersecurity and Personal Data Protection.

2.2.1 Cybercrimes and Cybersecurity Bill

The South African Cybercrimes and Cybersecurity Bill was drafted in 2015, introduced in the National Assembly, and published in Government Gazette No. 40487 on 9 December 2016. The Bill intended to protect the South African public from being targeted by Cybercrime offenders and increased the number of data protection laws in South Africa (Mabunda, 2021). It defines a number of cybercrimes and proposes a range of penalties for infractions. The offenses are under the second and third chapters of the Bill. The offenses relate specifically to the unlawful possession of data, the unlawful and intentional securing of access to data, the unlawful acquisition, possession, provision, receipt, or use of a password, and access codes or data on devices to commit cyber offenses in terms of the Bill (Ralarala, 2020 & Mabunda, 2021). The Cybercrimes and Cybersecurity Bill also makes provisions for victims to report any cyber-related issues. The Bill introduced structures such as the 24/7 Point of Contact (operating 24 hours), the Cybersecurity Hub, and nodal points to promote the reporting, investigation, and prosecution of incidents of cybercrimes (Mabunda, 2021 & Van Vuuren, Leenen & Pieterse 2020). All crime reports were to be investigated, and feedback was to be received.

They also accepted the convention on cybersecurity and the protection of personal information (Mabunda, 2021).

2.2.2 Critiques and Developments of The Cybercrimes and Cybersecurity Bill

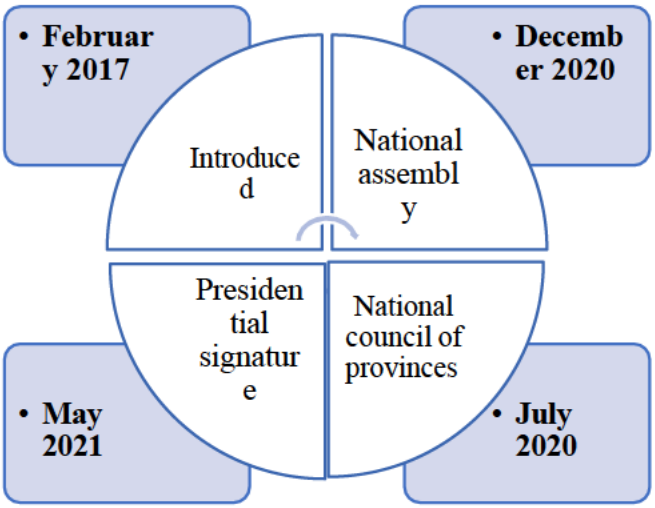
When the Cybersecurity Bill was drafted in 2015, the Department of Justice and Constitutional Development invited public comments on it, and many challenges were raised concerning, for instance, whether the bill adequately met the international standards set to combat cybercrime. According to Joynt (2023) and Reddy (2019), the bill was argued to be vague, limited the free flow of information, and gave the government too much power to police online activities. Furthermore, the bill was too restrictive and infringed on the rights entrenched in the Constitution of the Republic of South Africa, 1996, such as the right to privacy contained in section 14 of the constitution (Joynt, 2023). After considering all comments received on the Cybercrimes Bill 2015, the Cybercrime and Cybersecurity Bill was introduced in 2017. This bill was considered to bring a higher level of cybersecurity awareness to the business and the government (Govender, 2018). It offered approaches such as criminalizing several online activities and allowed for improved law enforcement agencies' power to investigate and combat cybercrime. The broad aim of the bill was to criminalize the unlawful and harmful distribution of data messages to provide for temporal protection orders. It aims to control jurisdiction concerning cybercrimes and gives powers to investigate and control aspects relating to mutual assistance with the investigation of cybercrime (Hofmeyr, 2020).

It was to provide for establishing a designated Point of Contact, provide proof of specific facts by affidavit, impose obligations to report cybercrimes, and provide for capacity building. It further provided that the executive may enter into agreements with foreign States. The bill also promotes measures to detect, prevent, mitigate, and investigate cybercrimes and to delete and amend provisions of specific laws (Kempen, 2019). The cybercrimes and cybercrimes bill of 2017 was also thoroughly scrutinized. The Bill was separated into two sections, one for "cybercrimes" and the other for "cybersecurity." The Bill was primarily criticized for its cybersecurity section, which raised concerns about the government's broad powers, including the possibility that it violated section 16 of the Constitution's right to freedom of expression. As a result, the Old Bill's cybersecurity elements were eliminated, and the name was changed to the 'Cybercrimes Bill,' which now exclusively deals with cybercrime (Cassim, 2011).

2.2.3 The Promulgation of the Cybercrimes Bill

The Cybercrimes Bill was signed into an Act of Parliament of the Republic of South Africa by President Cyril Ramaphosa on 21 May 2021. The Cybercrimes Bill does not define cybercrimes. However, it creates a series of offenses collectively referred to as cybercrimes (Boda, Dullabh & Steele, 2021). Figure 2.1 below illustrates the development and promulgation of the cybercrime bill in South Africa.

Figure 2.1: Cybercrimes Bill



Source: Boda, Dullabh & Steele, 2021.

Boda, Dullabh, and Steele (2021) mention the following **Objectives of the bill**:

- The Bill Provides that the Executive may negotiate with foreign states to promote cyber security.
- Impose obligations to report cybercrimes.
- Provide proof of certain facts by affidavit
- Establish a 24/7 point of contact.
- Regulate the power to investigate.
- Regulate aspects of mutual legal assistance
- Regulate the jurisdiction for cybercrimes.
- Provide interim protection orders.
- Prescribe penalties for cybercrimes.
- Criminalize the distribution of harmful data messages

- Create cybercrime offences.

There is a rise in crime as a service. The Bill mentions the following as cybercrimes committed unlawfully and intentionally (Boda et al., 2021 & Mtuze & Musoni, 2023).

S 2 –Unlawful access (if someone intentionally and unlawfully uses a computer system or data storage medium to put themselves or another person in a position to conduct an offense, that person has committed a cybercrime. Prohibits unauthorized access to computer systems and data storage devices).

S 3 –Unlawful interception of data (acquisition, viewing, capturing, copying)

S 4 –Unlawful acts in respect of software and hardware tools (use or possess)

S 5 –Unlawful interference with data or a computer programme (includes deleting, altering, rendering vulnerable, damaging, deteriorating, rendering useless or ineffective, obstructing, interrupting, or denying access to data or a computer programme).

S 7 –Unlawful acquisition, possession, provision, receipt, or use of password, access codes, or similar data or devices (purpose)

S 8 –Cyber fraud (anyone who intentionally and unlawfully misrepresents data or a computer programme, or by interfering with data or a computer programme, computer data storage media, or computer systems in a way that could actually or potentially harm another person is guilty of fraud. This involves posing as legitimate websites or asking for personal information via emails sent to victims).

S 9 –Cyber forgery and uttering (Forgery is the illegal act of intentionally manipulating data or a computer program to another individual's real or possible detriment. Cyber uttering is the illegal and deliberate dissemination of false information, such as computer programs or data, to defame another individual, either directly or indirectly).

S10 –Cyber extortion (crime committed by anyone intentionally and unlawfully commits, or threatens to commit, any of the offenses listed in sections 3 (1), 5 (1), 6 (1), or 7 (1) of the Cybercrimes Act with the intent to gain an advantage over another person or coerce another individual into performing an act or refraining from performing an act. Good examples of cyber extortion crimes are ransomware attacks).

S 11 –Aggravated offences (encompasses sections 3 (1), 5 (1), 6 (1), or 7 (1) with respect to passwords, access codes, or comparable data and devices.

An infringement or offender in this situation faces severe penalties if they are found guilty of an aggravated offense and can demonstrate that they knew or should have reasonably been suspected that the computer system is restricted).

S 12 –Theft of incorporeal property (patent) (A person is guilty of theft if they intentionally and unlawfully take moveable, physical property that either (a) belongs to someone else and is in their possession, (b) belongs to someone else but is in the perpetrator's possession, or (c) belongs to the perpetrator but is in possession of someone else and that person has a right to possess it that legally supersedes the perpetrator's right of possession, provided that the intention to possess the property includes the intention to deprive the person permanently)

2.2.4 Malicious Communications Include:

S 14 Data message that incites damage to property or violence.
S 15 Data message that threatens persons with damage to property or violence S 16 Data message of intimate image

2.2.5 Penalties

There are penalties for convicted offenders of cybercrimes. The cybercrime bills mention the conventions that an offender will face. These include fines and imprisonment for five to ten years, depending on the type of cybercrime and the severity of the offense. An offender may, for instance, receive a maximum of 15 years in imprisonment for aggravated offences (Boda et al., 2021) The Bill also allows for extensive penalties that could be imposed on anyone found guilty of cyber fraud, cyber forgery, or uttering, where a court will have the discretion to impose a penalty that it thinks suitable under section 276 of the Criminal Procedure Act 51 of 1977. A fine (unspecified), incarceration, a declaration as a habitual offender, and correctional supervision are all possible consequences of committing a cybercrime (Boda et al., 2021 & Hofmeyr, 2020).

In addition, the cybercrimes bill imposes obligations for businesses in South Africa, as well as Electronic Communications Service Providers (ECSPs) and financial institutions. ECSPs and financial institutions are held accountable for (a) cybercrime reporting and (b) preserving evidence relating to the cybercrime commission (Hofmeyr, 2020). Any ECSPs or financial institutions that fail to comply with these responsibilities may be found guilty of an offence and

face a fine of up to R50,000 if convicted (Hofmeyr, 2020). Businesses that may be victims of cybercrime or who, for example, have an employee who commits a cybercrime are expected to cooperate with law enforcement officials and aid them in any investigations they may conduct. Businesses may be obliged to comply with search warrants and/or court orders to provide details about computer systems involved in cybercrime and to preserve data or evidence relevant to a cybercrime investigation (Hofmeyr, 2020).

2.2.6 Protection Order

Protection order entails removing or restricting access to an electronic communication service provider whose electronic communication service is utilized to host or disclose the data message (Boda et al., 2021). This might happen when a complainant seeks a protection order under the Cybercrimes Act 2020. The order may also Prohibit disclosure or further disclosure of data messages related to the charge (Boda et al., 2021).

2.2.7 South African (SA) Jurisdiction

In the following cases, South African (SA) courts have jurisdiction to try offenders:

(i) If a person is arrested or an offence is committed in South Africa or onboard a vessel or ship, an installation, a fixed platform, or an aircraft registered in SA.

(ii) A person must be a citizen, a resident, and incorporated or registered in South Africa.

(iii) If the offence has an impact on a person, a restricted computer system in a public body, or a business in South Africa.

(iv) If there's an offence committed outside South Africa but against a citizen, a resident, a company incorporated or registered in South Africa, or a restricted computer system or government facility in South Africa (Boda et al., 2021).

Reddy (2019) further states that Crimes committed outside South Africa are guarded by Section 23 of the Cybercrimes Bill. Those crimes are trailed if they affect the Republic of South Africa. Crimes related to cryptocurrency are examples of crimes that cross jurisdictions. Therefore, extradition is a crucial tool in the prosecution of these crimes. Extradition processes ensure that the accused are returned to their original country upon the completion of the trial and to preserve the rights of such persons. This 'protection' involves ensuring adequate evidence to present a case warranting extradition.

Moreover, the Act elucidates that an accused can only be trailed for crimes committed, not additional crimes. Which means no other charge may emerge after extradition. The Budapest Convention of Cybercrimes as international cooperation guides cross-jurisdiction processes (Reddy, 2019 & Joynt, 2023). Cybercrime poses a challenge for legal enforcement as it transcends traditional jurisdictional boundaries, allowing perpetrators to be anywhere on Earth. To collaborate to combat cybercrime, the Council of Europe Convention on Cybercrime of 2001, also known as the Budapest Convention, is the only international instrument to address this issue. However, as technology and cybercriminals become more sophisticated, the convention may be outdated in addressing cybercrime (Joynt, 2023). Moreover, Reddy (2019) argues that law enforcement's use of international standards for criminality causes extra expenses in terms of time and resources. The Bill's Chapter 6 offers reciprocal support in investigating cybercrimes and evidence preservation; this applies in conjunction with Chapter 2 of the International Co-operation in Criminal Matters Act, 1996 (Reddy, 2019).

2.2.8 Powers to Investigate, Search, and Access/Seize

All criminal investigations start with the Criminal Procedure Act 51 of 1977 (CPA), which establishes the legal foundation for search and seizure operations. Nevertheless, one limitation of the CPA is that it does not include specific protocols for obtaining and protecting data from the internet (Reddy, 2019). A broad range of procedural authorities are mainly provided for police officials in Chapter 5 of the bill. These rules are intended to be utilized in compliance with section 35(1) of the CPA's procedural rules. The confiscation of "any weapon, instrument, or another article by means of which the offence in question was committed or was used in the commission of such offence" is allowed under Section 35(1). Standard Operating Procedures are also provided under the Cybercrimes Bill, specifically for acquiring and storing electronic evidence (Reddy, 2019). Section 40 deals with the conservation of evidence direction, while Section 39 expedites the preservation of data direction. A police officer or investigator may request technological support from electronic service providers, financial institutions, and individuals under Section 31(1) to locate, access, and seize an object. These rules are meant to support investigators in promptly identifying criminal activity, gathering intelligence and evidence, and analyzing retrieved evidence. Bringing criminals to justice depends on the powers of the South African police service (SAPS) and the Minister of State Security (Reddy, 2019)

2.2.9 South African Police Services (SAPS): Policing the Cybercrimes Bill

An office within the SAPS that deals with cybercrimes is imperative. The SAPS must adequately provide and maintain the designated point of contact. This means they must give urgent support to victims for proceedings and investigate crimes related to cybercrimes (Boda et al, 2021). SAPS recognizes that there is a constant need to provide a safe and secure information technology (ITC) environment for all South Africans. As a national law enforcement entity, SAPS is in line with the constitutional obligation to adopt and address the measures, policies, and/or strategies developed to deal with cybercrime (Kempen, 2019). The South African government is required by the cybercrimes bill's Chapter 10, Section 54, to ensure that the member of the Cabinet in charge of law enforcement must provide a sufficient human and operational capacity to detect, prevent, and investigate cybercrimes. They must provide basic training to members of the South African Police Service in the investigation of cybercrimes and, in collaboration with any higher education institution in the country or abroad, develop and implement accredited training programmes for members of the police service who are primarily involved in cybercrime detection, prevention, and investigation (Reddy, 2019).

Digital forensic experts are also particularly important in detecting and investigating cybercrimes. Law enforcement must possess information technology and computer forensic skills to prosecute cyber offenders successfully and ensure that no fabrication of evidence and data collected is rendered as inadequate evidence (Miller, 2023). However, Kempen (2019) argues that the role of the SAPS or state to combat cybercrimes effectively is still questionable. SAPS currently deals with cybercrime in an uncoordinated and fragmented manner. They lack a clearly defined, cohesive, and approved strategic framework for cybercrime. As indicated by the Electronic Crime Unit of South Africa, collaboration and guidance from other agencies such as the Federal Bureau of Investigations (FBI), Interpol, and the European Police Office (Europol) should be acquired as they are more skilled and established in the investigation of cybercrimes and/or computer related crimes (Reddy, 2019). There are further arguments that SAPS relies on other common law crimes to deal with cybercrime cases, such as fraud being perpetrated in the cyber domain or in terms of the limited offences created in sections 86 to 88 of the Electronic Communications and Transactions Act (ECT) 25 of 2002 (Kempen, 2019).

Dlamini and Mbambo (2019) also argue that although South Africa has taken a step forward in making the country more cyber-safe, it still faces challenges, especially regarding cyber security capacity skills. The government still lacks the knowledge and expertise to deal with cybercrimes. SAPS appears to be mainly directed by paper-based guidelines and strategies to deal with cybercrimes, and whether this challenge still persists or not is explored in this study.

2.2.10 The Electronic Communications and Transactions Act 25 of 2002 (ECT)

The Electronic Communications and Transactions Act (ECT) 25 of 2002 was also enacted in response to cybercrime in South Africa. Currently, the ECT Act's criminal legislation provisions serve as the primary statutory defence against cybercrime in South Africa (Maluleke, 2023). The ECT's primary goal is to ensure that electronic communications and transactions are made easier and more regulated for the public benefit (Maluleke, 2023). Case law from the past has also demonstrated the need for specific legislation to combat computer crime. Section 86(1) of the ECT Act is the first main section that makes any unauthorized access to or interception of data illegal. It substantially expands the list of forbidden actions to include interception of, in addition to, unlawful access and modification. Any unauthorized "interference with data," which would result in the data being modified, destroyed, erased, or otherwise rendered ineffective, is expressly forbidden by Section 86(2) (Nduka & Basdeo, 2022). Sections 85-89 of the ECT Act forbid and punish any activity related to unlawful production, sale, offer to sell, procurement, design, adaptation, or distribution of any device, including computer programs or components, with the intent to evade data protection security measures, computer-related fraud, and forgery, including attempts to aid and abet such crimes.

Cybercrime is covered in depth in Chapter 13 of the ECT. Punishable offences under the ECT, sections 86(3) and 86 (4) include anti-cracking and hacking laws, which prohibit the marketing, designing, and producing anti-security bypassing technologies. Sections 86(5) and 45 of the ECT deal with e-mail bombing and spamming, respectively, whilst section 87 deals with extortion, fraud, and forgery (Richards & Eboibi, 2021 & Nduka & Basdeo, 2023). Maluleke, (2023) notes that ECT is one of the most commended structures for cybercrimes. However, there is yet an opportunity for improvement. For example, the criminal sanctions under section 89 of the ECT have been criticized for being too ‘lenient.’ Most crimes prohibited by section 86 carry a maximum sentence of one year in prison.

In contrast, crimes prohibited by sections 86(4) and (5) (such as denial of service attacks) and crimes prohibited by section 87 (extortion, fraud, and forgery) carry a maximum sentence of five years in prison. However, the Regulation of Interception of Communications and Provision of Communications- Related Information Act 70 of 2002 (RICA) imposes stricter penalties (Richards & Eboibi, 2021). Moreover, the common law prevails in cases where the ECT does not include provisions for criminal punishment, according to Section 3 of the ECT. Other statutory remedies that are more effective in the prosecution of other types of cybercrime include Money laundering and other financially related offences prohibited under the Prevention of Organized Crime (Second Amendment) Act 38 of 1999 (POCA) and the Financial Intelligence Centre Act, 2001 (FICA). In addition, the Act established 'cyber- inspectors,' who are authorized to visit places to acquire information on cybercrime (under section 82 (1)). This provision, however, may violate sections 14 and 25 of the 1996 Constitution, which address the right to privacy and the property right, respectively (Richards & Eboibi, 2021).

2.2.11 The Protection of Personal Information Act (POPIA)

The Protection of Personal Information Act (POPIA) is another legislation enacted in 2013. The main aim of the Act is to address privacy rights (Ralarala, 2020). It seeks to protect information and data by addressing the issues of security, discrimination, and theft. The right to privacy, which is a constitutional right, is able to regulate and deliberate on various powers, duties, and functions, including monitoring and ensuring compliance by public and private bodies and handling complaints in respect of violations of POPIA (Ralarala, 2020). In other words, the Act guards which personal information is allowed to be processed legally by responsible parties and provides the rights of people to protect their personal information (Ralarala, 2020). The Information Regulator aims to investigate reports of violations of the protection of personal information or data, which includes subpoenaing individuals to appear before the Information Regulator, obtaining evidence, conducting private interviews, and, upon issuing of a warrant, entering and searching any premises and seizing information linked to the commission of an offence in terms of POPIA. The aim of the Bill and the POPIA is to expand and provide guidelines relating to data processing, protection, and privacy. It also aims at “bringing South Africa in line with international guidelines” (Maluleke, 2023).

2.2.12 The National Cybersecurity Policy Framework (NCFP)

The National Cybersecurity Policy Framework (NCFP) is another piece of policing cybercrime adopted by the South African Cabinet in 2012. The policy sets out measures and mechanisms for coordination across government departments and other agencies and its purpose is to establish a cyber environment that is safe and reliable (Ralarala, 2020). It also aims to facilitate the establishment of relevant structures supporting cybersecurity, ensure the reduction of cybersecurity threats and vulnerabilities, and foster cooperation and coordination between the government and private sector. To ensure a strong interaction between policy, legislation, and technology, it is to promote and strengthen international cooperation, build capacity, promote a culture of cybersecurity, and promote compliance with appropriate technical and operational cybersecurity standards. Furthermore, the policy framework is intended to promote capacity building, focusing especially on skills and research competence to ensure that South Africa's cybersecurity technical standards are at par with the global best practices (Ralarala, 2020).

2.3 International Legal and Regional Frameworks on Cybercrimes

One of the international or regional conventions on cybersecurity is the African Union (AU) Convention on Cybersecurity and Personal Data Protection. African states successfully negotiated and adopted the regional convention on June 27, 2014, during the 23rd session of the AU Summit in Malabo, Equatorial Guinea (Nduka & Basdeo, 2022 & Richards & Eboibi, 2021).

2.3.1 African Union: Convention on Cyberspace Security and Personal Data Protection

The convention was established by the African Union to respond to the cyber security challenges and gaps in Africa (Ralarala, 2020). It established a legal framework for cyber-security and personal data protection and embodied the commitments of African Union Member States to build a secure and safe cyberspace in Africa.

Under the AU Convention on Cybersecurity and Personal Data Protection, cybercrime is defined as**:**

- Any Attack on computer system.
- Computerised Data Breaches.
- Content-related offences.
- Offences relating to electronic message security. and

- Property Offences.

Chapter 3 of the Convention obliges State Parties to adopt appropriate and adequate measures to implement the national cybersecurity policy, especially legislative reform and development (Kempen, 2019). In other words, the African Union Convention requires signed parties or countries to provide legal instruments and policies to regulate and guide cybersecurity governance and reduce cybercrimes. Kempen (2019) states that the convention has been signed by 14 of 55 African Union states, whereas a minimum of 15 states are needed to sign it in order for it to come into force. Since its adoption, only a few countries have enacted distinct national cybercrime laws, while others have drafted cybercrime bills. Countries such as South Africa, Kenya, Botswana, Mauritius, and Zambia have cybercrime legislation in place, while eleven other states are developing or have started consultations to develop the required legislative instruments and policies (Nduka and Basdeo, 2022). The states that have ratified the Convention on Cybercrime as of December 28, 2020, include Senegal, Ghana, Mauritius, and Morocco.

Kempen (2019) states that more states need to be encouraged to abide by the convention and develop cyberspace necessary legislation to protect their citizens and promote and abide by the rule of law while also respecting human rights, such as the protection of personal information. Kempen (2019) further argues that users found guilty of privacy violations should be penalized without undermining the idea of the free flow of personal information. According to Turiansyi (2020), although AU states have established cybersecurity laws, there are still challenges with how the laws are worded and how the laws shift toward political stance instead of protecting the country's citizens. The author urges the AU to rectify the anomalies and encourages other AU members to sign and ratify the convention (Turiansyi, 2020). To reduce the risks associated with using ICTs, the African Union Convention also supports consultations, developing cyber diplomacy skills, and information and communication exchange between nations at the foreign policy level (Van Vuuren, Leenen, & Pieterse, 2020). It is believed that a unified approach must be encouraged to improve the regional, continental, and international collaboration required for cross-border cybercrime investigation and prosecution. This strategy, it is argued, will help African nations build a safe and resilient cyber environment by thoroughly understanding the dangers and vulnerabilities associated with innovative technology and the Internet of Things (IoT) in the future (Turiansyi, 2020).

Interestingly, evidence shows that the AU Commission has been cooperating with other international cyberspace organizations in collaborative ventures to ensure cybersecurity and safety globally. For instance, in 2018, the AU Commission joined forces with the Council of Europe to organize a cyber security and cybercrime policies workshop. The AU Commission also worked with the Internet Society to develop both privacy and personal data protection laws. This showed commitment and willingness from the different states to promote and develop the best practices to curb cybercrimes and provide security. Technology is advancing at a fast pace; therefore, governments must be able to respond to cybercrimes not only through legislation and policies but also through cooperation and collaboration. It is important that all states and citizens work together and engage in decision-making processes, as well as ensure clear roles and responsibilities for stakeholders, including governments, corporations, and citizens (Turiansyi, 2020).

2.3.2 Implementation of Cybercrime Strategies in Africa

Although many member states have yet to ratify the AU Convention, all African states are encouraged to adopt policies and legal frameworks to respond to cybercrimes. It is worth noting, however, that in line with AU's call for action, several countries, including Nigeria, Kenya, Zambia, Botswana, Malawi, Ethiopia, Tanzania, Cameroon and South Africa. have adopted policies and legal frameworks to respond to cybercrimes.

2.3.2.1 Nigeria

Nigeria is one of the African countries often targeted by cybercriminals due to its weak control and security measures (Maluleke, 2023, citing Schoeman, 2017). Although the policing of cybercrimes has been deemed necessary by law enforcement agencies, departments, and governments across the globe, Nigeria's response to cybercrime issues is still minimal, and the incidence of cybercrime is increasing. The increased cybercrimes continually challenge the Nigerian police force (Ismail, 2020). This is despite the evidence of interventions, particularly the establishment of the Economic and Financial Crimes Commission (EFCC) and the enactment of supporting legislations, such as the Advance Fee Fraud and Other Fraud Related Act of 2006 and the Cybercrimes Act of 2015 (Ismail, 2020).

While the former empowers the EFCC to handle online fraud, the latter aims to protect critical national information infrastructure, foster cyber-security, and safeguard computer systems, networks, electronic communications, data, computer programmes, intellectual property, and privacy rights. It also provides an efficient, unified, and comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, and prosecution of cybercrimes in Nigeria (Richards & Eboibi, 2021 & Shola, 2021). Part 111 Sections 5-40 of the Cybercrimes Act also forbids all crimes involving the use of computers and other electronic devices. It also aims to stop computer crimes by taking actions that compromise a website's cyber-security measures and violate an internet user's privacy (Richards & Eboibi, 2021). The Act forbids utilizing registered names or trademarks without permission, unlawful interception, computer phishing, spamming, malicious virus distribution, and purposeful access to computer systems or networks for fraudulent reasons. It also forbids pretending to be someone else (Identity theft), using passwords or electronic signatures without permission, and making up information to get electronic cards.

Other offences include child pornography, cyberstalking, cyberterrorism, racist speech, and xenophobic offences (Richards & Eboibi, 2021 & Shola, 2021). The penalty for these acts of crime can involve imprisonment, a death sentence, or a fine of $12,904 to $64,523, depending on the severity of the offence (Shola, 2021). Nigeria has also created a Cybercrime Unit under the Department of Investigations. Established in 2016, the Unit works with the Interpol National Centre Bureau, the police force headquarters, and other units. Further, law enforcement officers continually undergo special training to improve their capacity to investigate and prosecute cybercrime offenders effectively. Cybercrimes Reporting Portal has also been created to enable victims to report incidences of cybercrime online and allow the NPF to detect cybercrimes and their offenders quickly. Social media channels (such as Facebook, Twitter, and Instagram) have been used as surveillance and intelligence to catch cybercrime suspects. Cyber offenders in Nigeria are believed to be the major distributors of malware, scams, and phishing attacks, compromising about 150 states since 2017 (Ismail, 2020). The Nigerian police force also utilizes third parties to respond to cybercrimes. Third parties include private entities (such as banks, internet service providers etc) that are legally authorized to provide the police with any information about online crime activities. Through this collaboration and cooperation from private companies, many cyber offenders have been detected and convicted.

Furthermore, Kidnapping and ransom claim offences (using phones) from victims' families have been a challenge in Nigeria, which threatens the security of the public. The police use the Global Positioning System (GPS), Global Information System (GIS), and phone tracking to deal with offenders (Ismail, 2020).

2.3.2.2 Kenya

Kenya has several laws to respond to cybercrimes. In 1998, the Kenya Information and Communications Act (KICA) was adopted, and in 2008, it was amended and replaced by the Kenya Communications Amendment Act 2008. The aim of the Act was, and still is, to regulate electronic transactions and to provide guidance on what would be considered offences committed on the Internet (Ralarala, 2020). In accordance with the KICA, the Communications Authority of Kenya was founded in 1999 to facilitate the growth of Kenya's communications industry. A National Security Council has been established by Article 240 of the Constitution and is tasked with supervising all national security agencies in the Republic of Kenya. The KICA also led to the creation of the Kenya Computer Security Incident Response Team (CSIRT-Kenya), a component of the framework for national cybersecurity management. It comprises law enforcement organizations collaborating with the Communication Authority to handle cybersecurity issues on a global and local scale (Ralarala, 2020).

The Kenyan government also provides protection for national critical information infrastructure. The National Strategy, Policy, and Regulatory Framework Protects its national critical information infrastructure against cybercrime threats. They have the documents Kenya Vision 2030, National Cybersecurity Strategy, 2014, National Cybersecurity Masterplan, National Cybersecurity Framework, 2014, and Kenyan Information and Communications Technology Policy, 2006. Regulations and laws include the Information and Communications Act 2013, Cybersecurity and Protection Bill 2016, etc. (Gumbi 2018). In 2018, the Data Protection Bill was approved and adopted. It focused on the right to privacy. The bill, which safeguards personal data and governs how personal information is utilized, was officially enacted and adopted into law, The Kenyan Data Protection Act (KDPA), in 2019. Section 3 of the Act delineates the objectives and goals of the provisions, which include regulating the processing of personal data, ensuring that the processing adheres to the principles outlined in Section 25 of the Act, protecting the privacy of individuals, and facilitating the establishment of institutional and legal

mechanisms. The legal guidelines aim to protect personal data and safeguard the way their data is being processed and whether it is consistent with the Act. (Ralarala, 2020).

Kenya also has the Computer Misuse and Cybercrimes Act No. 5, 2018. The Act was passed to create a legislative framework to combat cybercrimes and to address the requirement for the establishment of organizations to prevent and detect cybercrimes (Richards & Eboibi, 202). The Act aims to:

- Provide for offences that relate to computer systems.
- Enable timely and effective detection,
- Prohibit, prevent, respond, investigate, and prosecute computer and cybercrime offenders.
- Promote international cooperation in dealing with computer and cybercrime challenges.

The Act looks at the following as a guide for offences (Richards & Eboibi, 2021):

- Unauthorised access to computer systems
- Access with intent to commit further offence.
- Unauthorised interference and interception.
- Illegal devices and access codes.
- Unauthorised disclosure of passwords or access codes.
- intentional manufacture, adaptation, sale, procurement for use, importation, supply, distribution of a device, programme
- Cyber espionage.
- False publications.
- Child pornography.
- Computer forgery.
- Computer fraud.
- Cyberstalking and cyber-bullying; and Offences committed through computer systems.
- Identity theft and impersonation,
- Phishing

Despite the advances made in Kenya's cyber security and safety regulatory framework, the Computer Misuse and Cybercrimes Act has been questioned for having imprecise definitions of what constitutes illegal behaviour. An example would be the prohibition of the use of hate speech. Furthermore, concerns have been raised about the precise scope of the government's monitoring capabilities and whether they would violate citizens' right to privacy and the Constitution. The Law Society of Kenya (LSK) is reported to have petitioned against the Act with concerns that it infringed on the Bill of Rights, the right to freedom. The criticisms pose challenges to enforcing the Act, and some observers believe that the Act needs to be revisited or amended (Ralarala, 2020 & Richards & Eboibi, 2021).

2.3.2.3 Zambia

Zambia is another state struggling to combat cybercrimes and/or internet fraud. In response to the rise in cybercrimes and online fraud, Zambia developed the Electronics and Communications Transaction Act No. 21 of 2009. The Zambian government also adopted the Computer Misuse and Crimes Act No. 13 of 2004. The Act aims to prevent any unlawful use, access, or interference with a computer, safeguard data security, integrity, and availability, stop computer system abuse, and make obtaining and using electronic evidence easier (Richards & Eboibi, 2021). Another intervention is the development of the National Policy Framework on Cyber Crime. This policy makes acts involving computer misuse illegal and punishable. However, Maluleke (2023) asserts that Zambia still lacks the organizational capacity, tools, and expertise to combat cybercrime effectively.

2.3.2.4 Botswana

In 2018, an Act to repeal and re-enact, with amendments, the *Cybercrime and Computer Related Crimes Act* of 2007, was adopted in Botswana (Maluleke, 2023). The Cybercrime and Computer Crimes Act No. 18 of 2018 listed several cybercrimes under sections 4-18 of the Act. Cybercrimes include but are not limited to breaching computer systems, gaining unauthorized access to computer services, breaking into computer systems with the intent to commit crimes, interfering with data without authorization, obtaining devices or data illegally, disclosing passwords or access codes without authorization, causing damage to computer systems, breaking into critical national infrastructure while committing crimes, cyber extortion, cyber fraud, cyberstalking, and offensive electronic communication (Richards & Eboibi, 2021 & Bande,

2018). The Act applies to any individual, regardless of citizenship, who commits cybercrime within or outside Botswana, affecting a registered ship or aircraft. It also grants jurisdiction to courts over nationals who commit cybercrimes outside Botswana if their conduct constitutes a foreign offence.

Other laws that deal with cybercrime, in addition to CCRC 2018, include the Telecommunications Act, the Electronic Record Evidence Bill, and the Criminal Procedure Act. To further safeguard Botswana's data and privacy, the Data Protection Act (2018) was also passed in 2018 (Richards & Eboibi, 2021). Although Botswana has put measures in place to fight cybercrime, corrupt practices impede the enforcement of the measures. For instance, the number of cases of falsifying identity cards and documents to withdraw cash from banks illegally is rising. The actions of corrupt government officials also exacerbate the challenges, such as the illicit sale of Botswana passports to foreigners. Due to these difficulties, according to some observers, law enforcement organizations and criminal investigators are expected to be resourceful in locating, arresting, and convicting cyber criminals. Furthermore, employee competency is critical to any organization's ability to combat cybercrimes. Hence, periodic cybersecurity training is imperative. For example, it has been observed that several insider security breaches in Botswana are caused by a lack of knowledge of security principles than just being criminal. Therefore, more sophisticated and technology-based tools are needed to effectively deal with cybercrimes (Richards & Eboibi, 2021).

2.3.2.5 Malawi

The World Economic Forum's 2010 study reveals that Malawi ranks 15th out of 133 countries for ICT networked readiness. The internet, however, presents security challenges, including a lack of cybersecurity skills and spam, draining scarce services, and posing risks to developing countries. Government entities and large corporations are at risk of cybercrime, with sophisticated cases affecting major corporations. However, legislation, experts, and educational programmes can enhance cybersecurity, raising awareness and addressing the issue of untrained and inexperienced users (Bande, 2018). In Malawi, the Electronic Transactions and Cyber Security Act number 11 of 2016 was developed to respond to and criminalize cybercrimes.

The act aims to criminalize offenses related to computer systems and information communication technologies, create provisions for electronic transactions, establish and operate the Malawi Computer Emergency Response Team (MCERT), provide provisions for the investigation, gathering, and use of electronic evidence, and address matters incidental to and connected to these actions (Bande, 2018). Apart from establishing explicit guidelines for data protection and privacy (included in sections 71–74), the Act also forbids and punishes several cybercrimes, such as unauthorized access, interception, or manipulation of data, Prohibitions against hacking, breaking into computers, introducing viruses, sending offensive messages online, engaging in cyberstalking, engaging in cyber harassment, and sending unsolicited emails. The Act prohibits data interception, punishing anyone who intercepts data without authority or permission (Bande, 2018 & Richards & Eboibi, 2021). To address the impact of information and communication technologies on national security, Malawi also implemented the National Information and Communications Policy in 2003. However, Despite Malawi CERT's existence, Richards & Eboibi (2021) argue that there are still issues, such as a shortage of skilled law enforcement officers and a computer security incident response team.

2.3.2.6 Ethiopia

Ethiopia has issued a proclamation that criminalizes crimes against computer systems and data to stop the spread of cybercrimes. The primary aim of the 2016 Computer Crime Act is to safeguard Ethiopia's political and economic stability (Degabasa, 2024). The Computer Crime Legislation of 2016 forbids unauthorized manipulation of data, unauthorized interception of private information, and unapproved access to computer systems. The Act also prohibits identity theft, fraud involving computers, and data falsification. The Public Prosecutor and the Information Network Security Agency are responsible for enforcing the legislation. Building capacity is essential for efficient enforcement, and the effectiveness of the legislation is dependent on the cybercrime-combatting capacity of judicial officials, security agencies, investigators, and prosecutors. However, the enforcement of the Act may be constrained by some observed weaknesses, gaps, and contradictions in its provisions. For instance, there are concerns that some parts of the law violate residents' right to privacy (Richards & Eboibi, 2021). It is also argued that the Ethiopian current legislative framework is inadequately adapted to technological advancements, as explained in the proclamation (Degabasa, 2024).

It fails to prevent, control, investigate, and convict those suspected of computer crime. Therefore, efforts to address these limitations are imperative, besides the ICT infrastructure and ICT-based services developed by the government to create a reliable cybersecurity and safety system.

2.3.2.7 Tanzania

Tanzania passed the Cybercrimes Act of 2015 to join other African countries in the response and fight against cybercrimes. The Act prohibits identity theft, unauthorized data trafficking, illegal access to computer systems, interception of private information, and interference with computer system operations (Richards & Eboibi, 2021). Section 6 of the Act makes it an offence to intercept non-public transmissions, non-public electromagnetic emissions, and non-public computer systems connected to one another. The definition of interception includes acquiring, viewing, listening to, or recording computer data communication (Bande, 2018). However, the Cybercrimes Act 2015 has been criticized for over-criminalizing and violating human rights, such as receiving unauthorized information or data without the intention to access it. Critics also argue that the definition of cybercrime should be more precise. They argue, for instance, that the Act must specify what a person must do or a device a person must possess unlawfully and/or what device is designed or adapted to commit an offence (Bande, 2018).

Some challenges also constrain the enforcement of the Act. The challenges include underdeveloped cybercrime combatting institutions and legislative framework, doubts about the commitment of the government to address cybersecurity and safety issues, the politicization of cybersecurity management, and inadequate financial and human resources. These challenges negatively affect law enforcement officials' ability to deal with cybercrimes sufficiently. An independent cybercrime authority and more funding for capacity building to equip law enforcement officials with appropriate skills and tools are required to deal with cybercrimes effectively. There is no doubt about forensic and technological advancements, and the need for specialized training of law enforcement officials and sophisticated tools has become apparent for cyber security and safety (Richards & Eboibi, 2021).

2.3.2.8 Cameroon

Cameroon is reported to be one of the African nations most impacted by cybercrime and was having difficulty coming up with a solution. One of the various legislative instruments developed to combat cybercrime offences is the Cybersecurity and Cybercriminal Law, enacted in 2010- The Law lists various cybercrimes such as unauthorized access, interception, data destruction, and system attacks (Richards and Eboibi, 2021). The country also has the Electronic Communications Law which aims to harmonize domestic criminal substantive law elements with cybercrime provisions. It provides the necessary procedural law powers for the investigation and prosecution of such offences and other computer system-related offences. According to Richards and Eboibi (2021), despite the existence of international and regional cyber instruments, as well as cybercrime law and other legislative instruments, cybercrimes in Cameroon are still on the rise. There are several factors constraining the effective implementation of the Law. The factors include low user knowledge, insufficiency of the legislation, lack of skills, evidence, monitoring activities, and anonymity of those who break the law. The lack of forensic labs further complicates the analysis and presentation of digital evidence in court. In order to prosecute cybercrime cases successfully, the government needs to address these.

2.4 Council of Europe Convention on Cybercrime (CECC)

The Council of Europe Convention on Cybercrime (CECC) and its Explanatory Report were adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest on 23 November 2001, and it entered into force on 1 July 2004 (Council of Europe, 2001). As of September 2019, 65 countries, including some African countries, had signed and ratified the Convention. The list of African countries that have signed and ratified the Convention includes Cote d'Ivoire, Ghana, Nigeria, Senegal, Morrocco, and South Africa. South Africa signed the Convention in 2011 (Nduka & Basdeo, 2022). The Convention provides guidelines for member states to develop comprehensive legal and institutional frameworks to combat cybercrime. It also promotes international cooperation between member states, global and regional bodies, and even non-member countries (Nduka & Basdeo, 2022).

The national convention on cybercrimes has been commendable in forming national laws that allow authorities to operate across national borders. However, it must be noted that there are still challenges when it is needed to be implemented. The CECC criminalizes the following computer practices (Gumbi, 2018):

- Criminalizes intercepting non-public computer data transmissions,
- Imposes corporate accountability,
- Demands the production of stored computer data,
- And encourages countries to cooperate in investigations.

Chapter II of the Convention recommends adopting measures to be taken by member states at the national level to combat cybercrimes. Section 1 of this chapter deals with substantive criminal law, focusing on punishable infringements relating to, for example, copyright and related rights, computer- related fraud, child pornography, illegal access, illegal interception, data interception, and computer forgery (Tosoni, 2018 & Gumbi 2018):

- Copyright infringements and related rights: stipulate that each party must take action under their national law to make the infringement of copyright and related rights a crime. This provision addresses offenses linked to copyright and related rights infringements.
- Computer-related Fraud involves any actions taken with the intent to cause property loss to another party by manipulating, deleting, suppressing, or tampering with computer data in order to obtain financial advantage for oneself or another fraudulently.
- Child pornography: criminal offences for actions that involve creating, disseminating, transferring, obtaining, and owning content that shows children or people who appear to be children participating in sexually explicit behavior.
- Illegal access: Such an offense, which entails using a computer system, may be perpetrated by breaking into a security system or with other dishonest motive that entails using a computer system.
- Illegal interception: involves the unlawful interception of computer data made by technical means, which include electromagnetic emissions from a computer system carrying such data.
- Data interference: involves tampering with data in a way that results in its purposeful destruction, loss, degradation, alteration, or suppression of computer data without authorization.

- Computer forgery entails the deliberate entry, alteration, or deletion of computer data to produce inauthentic data with the goal of using such data as legitimate information for legal purposes.

The major role of the CECC is to promote a shared criminal strategy aimed at protecting society from cybercrime, particularly through adopting suitable legislation and promoting international collaboration. Although the CECC aspires to foster international collaboration in prosecuting cybercrime, it makes no provision for network security cooperation. Africa is reported to be expanding faster than any other continent in terms of cybercrime. Expanding broadband connections across the continent has resulted in a rise in the number of people using the internet and, therefore, susceptibility to cybercrimes (Cassim, 2011).

2.4.1 Policies and Regulatory Frameworks Used in Western & European Countries to Curb Cybercrimes.

Various Western countries (such as the United States, United Kingdom etc) are in line with the standard of the European Council that seeks to address global challenges of cybercrimes and develop laws that seek to respond to and decrease cybercrimes.

2.4.1.1 United Kingdom (UK)

Every year, the UK Office for National Statistics publishes a Crime Survey. According to the survey, which was made public for the year that ended in March 2018 there were about 4 million cases of cybercrime in England and Wales. About 3 million of the estimated cases had to do with fraud, and the remaining 1 million were cases of computer abuse, which included hacking and child pornography. Additionally, there is proof that some types of cybercrimes are becoming more prevalent yearly. Hackers are developing increasingly sophisticated methods to carry out their illegal activities, placing the public in danger (Ralarala, 2020). The majority of jurisdictions in several Western and European nations have made cybercrime cases, such as misuse of computer tools and racism, xenophobia, and recruitment or exploitation of minors, illegal and subject to criminal penalties (Khan, Saleh, Dorasamy, Khan, Leng, & Vergara, 2023).

UK's Cyber Instruments:

To respond to cybercrimes, the UK has developed a number of cyber instruments. The list includes the Computer Misuse Act of 1990, the Communications Act of 2003, the Civil Contingencies Act of 2004, the Data Protection Act of 2018, and the National Cybersecurity Strategy of 2016–2021.

.

The Computer Misuse Act of 1990 aims to protect computer content from illegal access and modification (Khan, Saleh, Dorasamy, Khan, Leng, Vergara, 2023). The first section of the Act addresses unauthorized access to computer material. It states that it is illegal for anyone to command a computer to carry out any task that gives them access to computer data or programmes. The section continues to state that the person securing the access is not authorized to do so and is guilty of an offence (Gumbi, 2018). The second part of the Act addresses unauthorized access to computer systems, and anyone who does so with the intent to commit a crime or makes it easier for someone to do so commits an offense. Additionally, this section stipulates that the behaviour described in section one need not be carried out simultaneously with this behaviour or on the same occasion. It is sufficient to prove that an infraction has been committed if the intention was to commit the offence. Unauthorized alteration of computer content is made illegal in Section 3 of the Act. The person must possess the necessary information and the necessary intent at the time of the offence, which the provision defines as an intent to modify data in a way that damages the computer or computer programme (Ralarala, 2020).

The Communications Act of 2003's covers Electronic Communications Networks and Services. According to Section 125 of this Act, obtaining electronic communications services with the intention of avoiding paying a fee associated with using those services constitutes a crime. Additionally, possessing or supplying equipment with the intent to assist in the violation of Section 125 is illegal (Gumbi, 2018 & Ralarala, 2020). The Civil Contingencies Act of 2004 focuses on provisions for civil emergencies. Protection against cybercrime and the achievement of cybersecurity are pertinent to Section 19 of this Act, which defines crises and necessitates the establishment of backup plans. An incident that poses a significant risk to the United Kingdom's security, like a communications system failure, falls under this category (Ralarala, 2020 & Gumbi, 2018).

In 2018 the UK enacted the Data Protection Act to protect individuals from processing data that is personal and confidential (Ralarala, 2020). The Act was to bring the UK in harmony with the European Union's Charter of Fundamental Rights, which encourages member states to respect and protect citizens' right to personal and confidential data protection. The intent of the National Cybersecurity Strategy 2016–2021 is to provide a safe and reliable cyberspace in the U.K. The strategy aims to investigate and plan for understanding threats, combat cybercrime, manage incidents, establish active cyber defense, design cybersecurity features in technology, enhance government cybersecurity, and develop cybersecurity skills. The plan seeks to increase network security, control cyber risk, and create a skilled labor market (Ralarala, 2020). It must be noted however, that several of these cyber instruments were developed more than 20 years ago, and some may need to be updated in order to keep track of the dynamic cyber environment. Ralarala (2020) states that it was announced in 2018 that preparations were being made to establish courts with special jurisdiction over cyber fraud and economic crimes. This move was seen as a positive step in the battle against cybercrime. It will enable cases to be heard by presiding officers who are knowledgeable in cyber issues; and also make it easier to track case laws.

2.4.1.2 United States

The United States is among the first nations to enact federal and state legislation against cybercrimes. The country's earliest legal instruments include the Computer Fraud and Abuse Act of 1986 (CFAA) and the Electronic Communication Privacy Act of 1986 (ECPA). The former was developed to prohibit the use of internet-connected computers as tools for fraudulent activity while the latter covers the use of wiretaps in criminal investigations. This Act forbids anyone (including law enforcement officials) from making an unlawful intercept, revealing, or exploiting the material unlawfully intercepted. (Hosani, Yousef, Al Shouq, Iqbal & Mouheb, 2019). Further, the Children's Online Privacy Protection Act of 1998 (COPPA) was developed to establish guidelines to govern the gathering of children's personal information. Besides COPPA, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CANSPAM) was enacted to stop the fraudulent use of commercial email, also known as spam. Another legal instrument was the National Information Infrastructure Protection Act of 1996 (NIIPA), which was designed to strengthen the CFAA (Dlamini & Mbambo, 2019).

In 1996, the US Department of Justice developed the United States Code to respond to cybercrimes. This was an effort to stop illegal computer access that endangered the safety and well-being of people, as well as business and government agencies that depended on computers for communication. The Code punishes individuals who engage in fraudulent behaviour and associated computer-related activities by fining and/or imprisoning them on conviction (Dlamini & Mbambo, 2019). Hosani et al. (2019) state that laws deal specifically with cyber harassment (such as cyberstalking and bullying). The laws include the Interstate Communications Act of 2012 and the Interstate Stalking and Prevention Act of 1996. The Interstate Stalking and Prevention Act establishes different prison sentences for anyone who uses electronic communication technology to put someone in reasonable fear of death or serious injury or to cause emotional distress to an individual (Hosani et al., 2019). The Interstate Communications Act stipulates that any individual who extorts or transmits interstate or foreign commerce, communication that contains a threat to harm a person or property, damage a person's reputation, or kidnap a person may be fined or imprisoned for a maximum of two years, or both. The United States also developed the Cybersecurity Information Sharing Act of 2015, the Cyber Security Enhancement Act of 2002, the Cyber Research and Development Act of 2002, the Homeland Securities Act of 2002, and the Federal Advisory Committee Act.

2.4.1.3 Southeast Asia

Asian countries, including Indonesia, are also aligned with the Council of Europe's Convention on Cybercrime (Budapest Convention). Indonesia has seen an increase in cybercrime, compelling the country to develop legal instruments and strategies to regulate and control cybercrime and ensure cybersecurity and safety in Indonesia. The Electronic Information and Transaction Law (EIT) (Number 11 of 2008) (Anwary, 2022 & Khan et al., 2023), which was later amended to become law No. 19 of 2016, was the first law in Indonesia to address cybersecurity. However, because it only addressed illegal offenses in the country, such as commercial content theft, it was determined that it did not apply to cybersecurity. While offering significant legal protection for digital transactions, it was updated by GR 71 of 2019, which safeguarded the personal data and information of enterprises while ensuring the security of transactional systems. Furthermore, to stop any fraud using websites, this regulation recognized the legitimacy of websites (Gojali, 2023 & Anwary, 2022).

Malaysia also passed the Personal Data Protection Act 2010 to protect customer data and reduce cybercrime in the country's commercial sector. This Act covers all firm employees who are qualified to manage customer personal information or have access to such data regarding business dealings in Malaysia. The protection of the economy and eliminating cybercrimes have been made possible by Malaysia's law enforcement (Gojali, 2023). Furthermore, Law No. 25 of 2009 on public service, Law No. 34 of 2004 on the Indonesian National Armed Forces, and Act No. 15 of 2003 on crime eradication and terrorism are among the laws in Indonesia that promote cybercrime security (Anwary, 2022). Anwary (2022) states that official bodies and government agencies have also established and developed and implemented strategies and systems to respond to cybercrimes. Among these are statutory bodies such as the Directorate of Information Security, the Information Security Coordination Team, and the Indonesia Security Incident Response Team on Internet Infrastructure. These government agencies, among other things, are responsible for Indonesia's cyber security and safety; they operate under the administrative wings of the Ministry of Communication and Informatics. According to the Indonesian Institute for Digital Law and Society, public and administrative bodies can manage cybercrime issues. However, there is a need for a thorough administrative and legal framework to guide the institutions and regulate their activities to ensure good governance in managing cybercrime (Anwary, 2022).

2.4.1.4 China

China is one of the countries with the highest rate of cybercrime. According to a recent report, the number of cybercrime cases in China doubled, reaching 282,000 recorded cases in 2021. The report claims that cyber fraud was among the leading types of internet criminal activity (Slotta, 2023). Against the backdrop of this observation, China is one of the countries most advanced in communication and information technology and can develop tools and legal instruments to combat cybercrime and regulate China’s cyberspace. True to this assumption, China has developed a legal and administrative framework, which includes the Cybersecurity Law of the People’s Republic of China (Effective June 1, 1917) and the Personal Information Protection Law, passed by the National People's Congress in August 2021 (Belli, 2021). Laws and policies about protecting personal data include laws enacted by the legislature, court rulings, administrative rules, and industry standards.

China's Criminal Law and Cybersecurity Law regulate network and critical information infrastructure operators' collection, storage, transmission, and use of personal information. Reportedly, China's most comprehensive regulatory standard is the Personal Information Security Specification (GB/T 35273-2017), with a revised draft now being considered for adoption (Turianskyi, 2020). The Chinese Cyberspace Administration has also published a draft rule on car data security for public feedback. In October 2021, China adopted Ethical Specifications of Next-Generation Artificial Intelligence and opened a consultation on Draft Guidance on Security Assessments for Cross-Border Data Transfers. In June 2021, Beijing adopted the Data Security Law (DSL), which defines more stringent requirements for processing critical, core state, and sensitive data (Belli, 2021). The DSL extends data localization obligations, requiring data storage in national territory servers for "important data." Essential data, including economic development, national security, public interest, individuals' rights, and corporate interests, are subject to special security requirements and international transfer restrictions. These requirements and regulations, most likely inspired by Russia's data localization provisions of 2015, were already in the 2017 Cybersecurity Law (Belli, 2021), which, in conjunction with the Anti-Terrorism Laws, govern internet service providers' obligations to monitor, identify, and destroy all terrorism-related data (Turianskyi, 2020).

In 2020, China approved the Governance of the Online Information Content Ecosystem, which aims to regulate online content (Belli, 2020). According to Belli (2020: 9), “The Provisions define which categories of content are considered illegal, what content producers are encouraged to develop and publish, and an obligation to prevent the production of ‘undesirable’ types of content.” Encouraged content includes that which fosters “core socialist values”, the doctrine of the Communist Party, and “positive and wholesome” messages. Undesirable content includes sensationalist headlines, coarse and vulgar language, gossip, and content that fosters improper habits that minors might emulate. Also in 2020, China announced its willingness to launch a Global Data Security Initiative, but so far, this initiative has not gained meaningful traction.”

2.5 Investigative Processes and Development of Digital Forensics to Combat Cybercrimes

Cybercriminals can defraud anyone in the world, steal data, transfer funds across jurisdictions, and evade detection.

This means that investigators have had to keep up the pace at which the speed of technology is developed. They have to build and acquire new ways of responding to these crimes. Law enforcement authorities and governments have established cybersecurity and digital forensics units to investigate cyber incidents. New personnel are needed, such as digital forensic investigators with certain skills to track and capture cybercriminals (Mugisha, 2019 & Wu, Breitinger & O'Shaughnessy, 2020). Indeed, Van Vuuren et al. (2020) states that These skills are needed for the forensic analysis of electronic evidence and a successful investigation and prosecution of cyber offenders. Wu et al. (2020) argue that more practical rather than theoretical measures are needed to combat these crimes.

However, there seem to be limited units in law enforcement that deal with digital evidence. Numerous reports of breaches involving financial and personally identifiable data have been made in South Africa. This exposes a lack of proper digital forensic readiness and incident preparation for cybersecurity (Bankole, Taiwo & Claims, 2022). Van Vuuren et al. (2020), however, state that countries such as the Ivory Coast have taken steps to establish special forensic police units. These units comprise law enforcement officers, forensic computers, telecommunication experts, and law consultants to assist in preventing and fighting against cybercrime (Van Vuuren et al., 2020). The use of digital forensics tools and techniques provides rich information on attack patterns, the workings of these criminal organizations, their goals, the latest tactics and tools they are employing, and more. Threat intelligence databases, as well as knowledge and best practice resources, benefit significantly from this proof. Additionally, if a corporation discovers that a breach has occurred, the evidence gathered from a digital forensic study aids in incident response and remedy efforts. Information on novel attack pathways and types of malwares that may not have been observed previously can also be discovered (Mugisha, 2019).

2.5.1 Scientific Evidence and Digital Forensics Investigations

Digital forensics is the process of locating, gathering, examining, and summarizing data from computers, mobile devices, and networks. Such data is often acceptable as evidence in court (Mugisha, 2019 & Kazaure, Jantan & Yusoff, 2023).

Digital devices used in the course of a cyberattack or defence also often provide evidence of many kinds of crimes, such as fraud, drug selling, human trafficking, assault, and murder.

Not only is digital forensics useful in commercial, private, or institutional organizations, but digital forensics is also essential for law enforcement and investigations. Digital traces are left by every action taken on a person's computer system and on a business network. These traces can be anything from cookies and web browsers, history caches to document metadata, erased file fragments, email headers, and more (Mugisha, 2019).

Previously, digital investigations had focused on computer systems and servers. However, technological advancement has seen the need to expand the application of forensic investigations to other devices such as cell phones, networks, cloud platforms, and the Internet of Things (IoT) (Al-Dhaqm et al., 2021). Al-Dhaqm, Ikuesan, Kebande, Razak, Grispos, Choo, Al-rimy, and Alsewari (2021) argue that for criminals to be prosecuted, scientific evidence that is reliable and relevant to crime must be admissible in a court of law. Without scientific evidence, linking a potential offender to a cybercrime is impossible. Therefore, forensic investigators have applied digital forensic investigation techniques as a means to an investigative process and prosecution of cyber criminals (Baror, Ikuesan & Venter 2021).

In digital forensic investigations, electronic data is gathered, examined, and preserved as proof in court. This type of work is frequently employed to detect cybercrimes such as online fraud, hacking, and data breaches. The process involves:

- Identification: This entails the establishment of the parameters of the inquiry and identifying any possible sources of digital evidence.
- Preservation: Protecting the digital evidence by ensuring its validity and integrity and stopping any data tampering, removal, or destruction.
- Gathering: Gathering digital evidence via imaging hard disks or copying data from other devices, both of which are forensically sound methods.
- Analysis: This entails examining the digital evidence to find pertinent details about the cyberattack, including its type, the name of the perpetrator, and the amount of damage it did.
- Presentation: Summarize the investigation’s findings Clearly and effectively so they may be admitted as evidence in a court of law (Kazaure et al., 2023):

The court can consider the findings if the investigations are conducted using scientific procedures.

Digital forensic investigations must produce credible evidence in order to survive legal scrutiny. An investigation's main goal is to learn more about a recent occurrence and identify a possible root cause to ensure it can survive judicial examination. Care must be taken to guarantee that the evidence's reliability cannot be questioned. This procedure calls for certain equipment, methods, and knowledge (Kazaure et al., 2023).

2.5.2 The Methods and Instruments in Scientific Evidence

1. The Collection of Evidence

The most important part of any investigation in forensic science is proving that the evidence being provided is real and has not been tampered with (Baror et al., 2021). The first responder needs the right authorization to look for and gather evidence at an electronic crime scene, such as plain view observation, consent, or a court order. To obtain evidence, the first responder must determine the legal justification for doing so. If this is unclear, they should adhere to agency protocols, speak with a supervisor, or contact the prosecutor. Care must be taken while handling digital evidence to protect the data and the physical device's integrity (Mugisha, 2019). Specific digital evidence necessitates unique methods for gathering, packing, and shipping. Electromagnetic fields, produced by magnets, radio transmitters, static electricity, and other devices, can corrupt or change data. Devices such as mobile phones and smartphones should be secured and blocked from receiving or transmitting data once they are recognized and seized as evidence (Mugisha, 2019). Kazaure et al., (2023) maintain that this procedure needs both technical and legal expertise for evidence to be legally sound. Social media is another valuable source of evidence. The initial studies on social media forensic extraction concentrated on identifying and recovering device-specific traces that web browsers and social network apps ignored. Acquiring pertinent information, gathering metadata, and verifying data integrity are all part of forensic social network collection.

2. Analysing Data/ Evidence

Cybercrimes such as cyberbullying and defamation on social media have been identified using sentiment analysis. Cyberbullying detection systems based on keywords have been presented, and hostile conduct is identified by combining natural language processing techniques with user behaviour. Methods for monitoring illicit behaviour and criminal tendencies on social media platforms such as Facebook and Twitter are also employed.

The difficulties associated with multi-tenancy and virtualized contexts make the gathering and examination of online social media information essential (Kazaure et al., 2023).

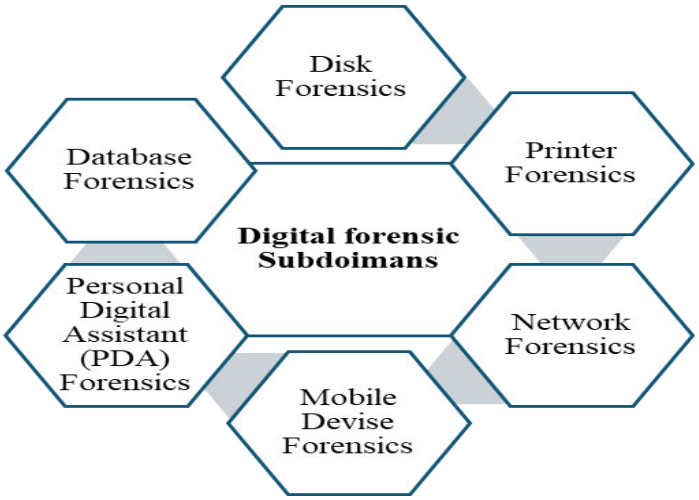
2.5.3 Digital Forensic Sub-Domains

Academic researchers have also been a part of the development of cybercrime investigation processes to support forensic investigators in their investigations. Investigative processes developed by academic researchers look at two domains: proactive forensic and behavioral biometrics (Al-Dhaqm et al., 2021). Proactive forensics looks at the deterrence of cybercrimes prior to the cybercrime incident. It suggests that cybercrime measures can be implemented, and evidence collected before the crime occurs. Behavioral biometrics involves the process of recognizing, extracting, and presenting a user's soft qualities from a digital object in a way that makes it easy to attribute an action or sequence of actions to a particular individual. Behavioural biometrics offers a method for producing behavioural characteristics of digital artifacts to allow for their forensic preservation for digital investigation (Al- Dhaqm et al., 2021).

According to Al-Dhaqm et al (2021), this method is becoming more widely used in digital forensics. Behavioural biometrics may be implemented into any subdomain, which makes it a potentially helpful component. User-initiated network packet requests, network traffic consumption patterns, and network load characteristics are all parts of behavioural biometrics in the context of the network domain. The usage consumption and patterns can be retrieved for forensics in computers, mobile phones, databases, and software, particularly for locating a software developer's fingerprint and distinctive coding sequence (Al-Dhaqm et al., 2021 & Pandey, Tripathi, Kapil, Singh, Khan, Agrawal, Kumar & Khan, 2020).

Mugisha (2019) further mentions several specialized branches in digital forensics that deal with cybercrimes:

Figure 2.2: Branches in Digital Forensics



Source: Mugisha, 2019

2.5.3.2 Disk Forensic

The first one is the Disk Forensics**.** Disk forensics is extracting forensic information from digital storage media like hard disks, USB devices, FireWire devices, CDs, DVDs, flash drives, and floppy disks. The first step in disk forensics is identifying the crime scene's storage devices. Computers may contain hard disks for IDE/CD, DVD, mobiles, PDAs, flashcards, SIM, USB / Firewire disks, magnetic tapes, zip drives, etc. When the digital evidence is located, it should be obtained using a forensic imaging tool. Bit-stream imaging is the process of attainment (Mugisha, 2019). Imaging must be performed using accurate and comprehensive data while preserving the disk geometry. The source media ought to be write-protected during this procedure. Following imaging completion, it must be compared to the original. Hashing is a technique to demonstrate that a copy is a replica of the original and has not been changed. After collecting the evidence, it must be safely stored and secured. The copy of the evidence must be stored in proper media or reliable mass storage. The evidence must also be analysed. The analysis process involves finding pertinent information in the digital evidence (Mugisha, 2019).

The analysis must encompass all available data, leaving no details omitted. Files and data in common folders, registries, pictures, databases, cookies, temporary files, swap, Internet history, passwords, and ambient data areas such as deleted, formatted, slack, unallocated, and lost can all be searched lastly the findings must be reported. The last step in disk forensics, report generation, is crucial. The way the evidence is presented will ultimately determine its value.

The report's technical evidence should be presented clearly and concisely so that even non-technical readers may grasp it (Mugisha, 2019).

2.5.3.2 Printer Forensics

For law enforcement and intelligence organizations, identifying the type of device that printed the document in question is extremely helpful. For instance, counterfeiters frequently employ color laser and inkjet printers after digitally scanning cash to create fake notes. Forgers create counterfeit passports and other documents using the same techniques. Investigators must establish that a certain printer brand and model was used to manufacture a forged bill or document. In addition, it is important to know precisely which printer was used, not just the type. This is done by examining a document to find the distinctive features of every printer and, secondly, by intentionally building printers with distinctive features (Mugisha, 2019).

2.5.3.3 Network Forensics

Network forensics is the process of collecting and analysing raw network data as well as methodically observing and monitoring network traffic to determine how a cyberattack occurred. WireShark, Network Miner TCP Dump is a common tool used in the process and ensures data collection and non- manipulation of data. It also features a response feature to warn users of potential dangers (Pandey et al., 2020). Professionals frequently utilize these technologies to investigate network breaches. Investigating infractions after the fact is beneficial in figuring out how they happened. To perform a comprehensive digital investigation and create a documented chain of evidence, a digital forensic investigator would collect network-based evidence from a specific computing device within the network so that it might be submitted in court (Mugisha, 2019).

2.5.3.4 Mobile Device Forensics

The science of retrieving digital evidence from a mobile phone using recognized techniques and under forensically sound circumstances is known as mobile phone forensics (Mugisha, 2019). The use of cell phones has increased dramatically, and the designs of cell phones are constantly changing due to advancements in current technology and the introduction of new ones. Cybercrime attacks have increased at the same speed. Knowledge about cell phone parts and construction is essential to comprehending the nuances involved in handling them forensically (Pandey et al, 2020).

Similarly, as cellular networks save usage logs and other data, they are a crucial component of cell phone forensics. Other tools used in mobile forensics include access data, FTK imager, and encase. Analysis of the SIM card and the phone's memory are included in cell phone forensics, each calling for a different process. Instead of concentrating on the detailed recovery of erased data, investigations typically focus on basic data such as calls and communication from SMS/Email (Mugisha, 2019 & Pandey et al, 2020).

2.5.3.5 Database Forensics

Database forensics is a subfield of digital forensics that deals with forensic investigations using standard investigative procedures and methods on database contents and metadata. One technique used in data forensics is called data carving. It is the process of extracting files or data from their raw fragments (Pandey et al, 2020). Additionally, a server's RAM may include cached data that has to be analyzed live (Mugisha 2019). Database forensics is a crucial field for identifying, detecting, acquiring, analyzing, and reconstructing incidents (Alhussan, Al-Dhaqm,Yafooz , Emara , Razak & Khafaga, 2022).

2.5.3.6 Personal Digital Assistant (PDA) Forensics

PDAs are becoming more widespread in the modern world. They are no longer the scant electronic devices that once held an address book, appointments, and personal data. In addition to the typical personal information management functions, modern PDAs combine wireless, Bluetooth, infrared, WiFi, mobile phones, cameras, global positioning systems, the Internet, and more. PDA-related crimes are more difficult to investigate than those involving traditional computers. This is primarily because these gadgets are more petite, require batteries, and use volatile memory to store data (Mugisha, 2019). A methodical approach and reasonable forensic procedures are required to gather such evidence and guarantee its acceptability in a court of law. Investigations into digital crimes significantly benefit from using a standard PDA forensic model, which offers an abstract framework for reference since they are frequently the first to respond to any computer crime in a business. in addition to law enforcement officials, such a model can benefit IT auditors, information security specialists, IT managers, and system administrators (Mugisha, 2019).

2.6 Recent Development in Cybercrime Responses

Organizations and people are exposed to serious hazards from cybercrime, but the cybersecurity sector has developed strategies that reduce those risks. Artificial intelligence (AI) and machine learning (ML) are among other recent advancements in mitigation techniques. It has improved cybersecurity by enabling security professionals to immediately identify and respond to possible threats by finding patterns and abnormalities in network data (Kazaure, Jantan, Yusoff, 2023). They enhance cybercrime detection because AI and ML can learn from data and adapt to new threats. Flexibility is provided by cloud-based security solutions, which enable businesses to monitor and safeguard their systems from any location. Distributed ledger technology, such as blockchain, makes the Internet safe and decentralized, making it more difficult for hackers to launch assaults. Additionally, it guards against fraud and safeguards transactions, which is why companies are drawn to improving their cybersecurity infrastructure.

In recent years, multi-factor authentication has become more popular, requiring users to submit various kinds of authentication (Kazaure, Jantan, Yusoff, 2023; Nnaemeka, 2023 & Chudasama, Patel, Shah & Shaikh, 2020). Threat intelligence, zero trust security, next-generation firewalls, endpoint detection and response, security orchestration, automation, and response are some strategies used to mitigate cybercrime. Zero trust security entail's strong identity verification and access controls for all users. The threat intelligence gathers and analyses data to identify and alleviate cyber-attacks. Endpoint detection and response systems identify and address endpoint threats, whereas next-generation firewalls integrate cutting-edge security capabilities with conventional technologies (Kazaure, Jantan & Yusoff, 2023).

2.7 The Effectiveness and Challenges of Existing Police Systems in Dealing with Cybercrime.

Gumbi (2018) argues that although there has been some progress in measures and the development of cybercrime laws, the legislation is still not adapting fast enough to effectively deal with new and increasing types and methods of cybercrime. A major challenge is locating the cyber offenders, let alone prosecute or convict them. Hackers or cyber-offenders appear to be highly skilled and make millions through cyber-attacks, while very few governments possess the technical skills and resources to deal with these offenses (Capazorio & Hollis, 2017).

Baylon and Antwi-Boasiako (2017) state that the growing internet infrastructure is also causing challenges for law enforcement and is making it easier for cybercriminals to carry out their illicit activities and enables them to swiftly and inexpensively send a large number of emails to a worldwide pool. Offenders are not only able to target victims in nearby places but can also target victims abroad.

Cordero and Thaw (2020) highlight that African nation's laws are still unable to broadly and uniformly criminalize internationally recognized cybercrime conducts, nor are they in line with those of the international community. The advancement of technology in developing countries is still increasing at an alarming rate, while structures needed to curb cybercrime are still lacking. This can mean more opportunities for offenders to attack the unprepared, lacking, or weak security systems put in place by governments and businesses. According to Gumbi (2018), South Africa's cyber laws need revision to criminalize crimes using intangible data, examine procedural regulations for thorough investigations, and ensure all victims and internet service providers report cybercrimes.

2.7.1 Regulatory and Legal Frameworks Challenges

Świątkowska (2020) highlights the importance of strong legislative and strategic frameworks in the fight against cybercrimes. However, there are evident challenges in some regions of the developing nations. Eoyang et al. (2018) and Orji (2021) state that the institutional capacity for cybercrime law enforcement, legislative and policy frameworks developed to respond to cybercrimes are inadequate. Cordero & Thaw (2020) support this statement and state that the existing legal frameworks in Africa and executive structure are insufficient for cybersecurity challenges in a technologically advanced society. According to Świątkowska (2020), out of 54 African nations, 30 lacked explicit legislative provisions on cybercrime and electronic evidence by 2016. Cybercriminals look for safe havens in underdeveloped nations hoping that weak laws and ineffective enforcement will lessen the likelihood of being caught and prosecuted. One of the leading causes of this issue is a lack of legislation and ineffective enforcement measures. The insufficient and unclear laws make it difficult for police, prosecutors, and judges to determine their application. For example, The Economic and Organised Crime Office Act, which investigates economic and organized crime in Nigeria, does not specify which cyber offences are included and/or considered as offenses.

Furthermore, The Electronic Transactions Act intended to facilitate electronic communications defines specific cyber offences but does not specify procedures for ensuring electronic evidence integrity and admissibility. This results in conflicting interpretations of the law regarding cybercrime among the police, prosecutors, and judges. (Baylon & Antwi-Boasiako, 2017). Furthermore, Świątkowska (2020) states that many developing nations still lack national cybersecurity policies that would offer a broad governance framework for long-term initiatives. This makes it more difficult to establish important roles and duties or to build a robust cybersecurity ecosystem. When there is no strategic direction, the fundamental tools for cooperation are frequently absent. Similarly, essential procedures such as those about information sharing, incident management, and national risk assessment are lacking (Świątkowska, 2022). African countries often struggle to uphold their domestic legal commitments under international law. An international legal framework for the investigation and prosecution of cybercrime is necessary to investigate, discourage, and impose legal punishments on cybercriminals.

Law enforcement officers are obligated to respect the actual boundaries of municipal, state, and federal jurisdiction and sovereignty. Getting information from other nations can be difficult, especially if it is needed urgently. This is especially true if the other country is in a different time zone, has a different legal system, lacks qualified experts, and speaks a different language (Maluleke, 2023). As a guide for international laws, the Convention on Cybercrime (CECC) of the Council of Europe has been developed and is crucial for uniformity in cybercrime laws. However, Maluleke (2023) states that creating computer crime legislation is costly. Before the Convention can act as a deterrent, a number of governments still need to ratify or sign it. Africa is becoming more aware of cybercrime due to inadequate regulatory frameworks and IT ignorance. African nations should approach the adoption of laws in a balanced manner (Maluleke, 2023). They must establish national legal frameworks that include suitable criminal legislation and domestic criminal procedural powers (Świątkowska, 2020). They must also improve their capabilities to detect, handle, and prosecute cybercriminals. Judiciaries must advance their knowledge of the cybercrime environment and understand the technicalities of cases (Leenen & Pieterse, 2020).

2.7.2 Jurisdiction and Cross-border Challenges

There are also Jurisdiction and cross-border issues that law enforcement agencies encounter in their fight against cybercrimes. Jurisdiction refers to a country's right to regulate and punish conduct. However, this right is often limited by physical boundaries. Establishing jurisdiction in cyberspace is a major challenge in enforcing cybercrime legislation, especially for African countries dealing with cases that cut across multiple countries (Ndubueze, 2020). Physical proximity between the victim and the perpetrator is unnecessary for cybercrime. Because of jurisdictional challenges and the increased resources needed to track down cybercriminals across national borders, criminal laws governing cyberspace typically result in few prosecutions. The 'love bug' virus is an example of how global cybercrime has caused issues and how cyber laws are a necessary precondition for investigation and prosecution (Gumbi, 2018). Cybercrime's cross-border dimension is an issue due to how states treat their criminal law as an expression of sovereignty, providing a powerful tool for social control that protects victims and limits individual rights. National cultural conceptions of deviant behavior often shape criminal law, and its scope depends on differing constitutional laws. Cyber activity is an inherently cross-border phenomenon, with data transfer processes taking place in multiple countries and critical infrastructures being integrated into computer networks, making and exposing anyone a target of cybercrime (Mabunda, 2021).

Through the internet, cybercrimes like computer fraud and defamation are readily planned and executed from outside. But looking into and upholding the law overseas is counter to national authority. Countries frequently provide mutual legal help to one another in order to get over this obstacle, particularly with extradition, which typically necessitates double criminality. This means that a suspect may only be extradited from one state to another to face charges for a crime they committed there if the extraditing state has laws against identical offenses. This idea can stop a suspect from being extradited from one nation to another to face accusations of creating malware. Furthermore, offering mutual legal assistance through formal channels may take too long for successful investigations and law enforcement, as traffic data may be deleted and procedures to obtain evidence from another country can take weeks or months (Mabunda, 2021).

- Positionality and Anonymity

One of the challenges that police face is the issue of positionality.

International criminal law requires that when an offence occurs in a specific state or country, it must be trialled there. When an offense is reported, the police must determine where the offense occurred, what type of offense, and whether it is regarded as a violation of law under the specific national legal framework (Gumbi, 2018). This can present difficulties for law enforcement as the crime can be committed within a particular area by an offender, and the effect of the crime felt in another area. Issuing arrest warrants, preparing a case for trial, and overcoming conflict of laws can be almost impossible for police. The laws concerning cybercrime activities seem to lack the principle of universality. Therefore, opening grounds for cyber offenders to violate victims without any accountability (Gumbi 2018 & Mabunda, 2021). Furthermore, finding a link between a suspect and the technological device used to commit an offense can be challenging. The police must prove that when the offense occurred, the suspect controlled the device, who, therefore, intended to commit the crime. Criminal activities may become widely spread across the globe in both time and space.

This may render the investigation ineffective as the victim and offender may not reside in one country, and the evidence needed to continue the investigation may be found in another country. This also poses difficulty for law enforcement or legal frameworks in determining the modus operandi of cyberspace crime (Mabunda, 2021). There are also issues presented by anonymity. The anonymity feature of the internet can sometimes be problematic and raise danger. Nevertheless, people may create new identities online because it's a non-linear, global space. Some contend that anonymity needs to be preserved by law to promote responsibility. Nonetheless, there has been a rising movement toward more online anonymity, which is essential in a constantly developing setting and opening to the broader public. Because of the socializing of the internet, illicit encounters are now more common (Mabunda, 2021). Świątkowska (2020) is of the view that States need to implement both substantive and procedural legislative measures to prevent and combat cybercrime effectively. However, Establishing and sustaining effective criminalization can also be challenging. Setting up regional processes is the first step; legal frameworks must remain adaptable and flexible. The primary challenge and fundamental issue in the fight against cybercrime is the transnational or cross-border nature. Victims and perpetrators are often located in different legal jurisdictions. Thus, those issues can only be resolved if efficient channels for cooperation and national legal system alignment exist.

Therefore, creating strong procedural powers and harmonizing aspects of national criminal laws related to cybercrime are necessary for an intense international collaboration against cybercrime. The fact that traditional cooperation instruments, such as mutual legal aid regimes, are clearly inadequate in the digital age further complicates the issue of cooperation. As a result, the international community must find new means of support (Świątkowska, 2020).

2.7.3 Security Systems Challenges

Governments acknowledge the need and respond to citizens' adoption of social media and technology for social and political change. According to a 2013 Symantec Corporation report, cybercrime is rising quickly in Africa, with many of the continent's nations being particularly vulnerable because of their weak network and information security, as well as their large number of domains (Turianskyi, 2018). According to Turianskyi (2018), law enforcement agencies cannot adequately respond to cybercrimes because strategies to prevent cybercrime are frequently out-of-date or unclear. Furthermore, Governments have too much discretion regarding security regulations and how they interpret national security, making it difficult for them to enforce the law. The comprehensive laws also lead to convictions based on alleged misconduct or defamation (Turianskyi, 2018).

The UN Economic Commission for Africa (UNECA) has discovered that although many African nations have put out legislation to tackle cybercrime, there is a lack of security system implementation in both the public and private sectors. Many organizations have experienced major financial losses due to cybercrime. Although many of these organizations are aware of online crimes, they lack a comprehensive understanding of what major impacts could be felt. This is also evident in the poor security systems organizations currently employ. They avoid paying for proper designs or systems to curb cybercrime as they consider it too costly (Turianskyi, 2018). Old, unlicensed, poorly managed, and inadequately secured information assets are major causes of cybercrime. Up to 80% of African computers are infected with malware, and Windows 7 is the operating system most susceptible to WannaCry attacks. Due to a lack of investment in security solutions and fundamental security measures, over 95% of African enterprises function below the line in terms of security and cannot handle cyberattacks. Upgrades and security updates are impossible since 57% of software used in Africa and the Middle East is not licensed.

Emerging economies often lack the latest software and hardware versions, making them vulnerable to attacks (Świątkowska, 2020).

Cybersecurity experts' concerns are that broadband services are opening in the continent, which means more users would be able to access the web, translating into more viruses and spam from online. As more people have access to these gadgets and can access or connect to the web, so will cybercrime and the number of victims increase. Cybercriminals always take advantage of the weak and vulnerable in the information and communication technology systems (Ndubueze, 2020 & Świątkowska, 2020). There is another aspect to this issue, which is that ICT providers frequently modify their goods to better suit the needs and expectations of their customers in order to meet market demands. High-security items are too expensive for many poor nations; as a result, producers provide less secure, yet still affordable, versions of their products. Cybercriminals can easily prey on such antiquated and vulnerable systems, using them as targets for direct exploitation to facilitate crimes (Świątkowska, 2020). Because billions of linked devices are being used by expanding populations, cybersecurity concerns in developing nations may have an impact on the entire world. These gadgets can be utilized in additional cyberattacks and are targets for cybercrime. The spread of unsecured devices has the potential to create bigger, more destructive botnets, which could seriously harm networks and businesses. One million hosts might form a botnet that could take down a fortune of approximately 500 corporations (Świątkowska, 2020).

2.7.4 Internet Access, Privacy, and Human Rights Challenges

It is difficult to strike a balance between Internet freedom and cybercrime prevention since technology advances faster than laws. The digital age was expected to promote openness, freedom, and democracy. However, authoritarian states (such as China) have used technology as a way to silence dissidents and use the internet for propaganda. Due to security concerns, they also restrict citizens' access to social media sites (Turianskyi, 2020). The rise of fake news and information warfare has exploited this, resulting in attacks and physical harassment. Governments need to balance legislation and regulation to protect citizens from cybercrime without infringing on online freedoms or allowing security services to spy on citizens.

To safeguard individuals against cybercrime, governments must provide a balance between legislation and regulation without restricting online access or allowing security services to invade the privacy of citizens (Turianskyi, 2020). Due to ideological differences, global cooperation on internet freedoms, personal data protection, or privacy is often difficult. China's 'cyber sovereignty' idea may lead to citizens being cut off from global internet services. Existing data laws vary internationally, with some countries requiring data storage and processing within their borders and other countries having better privacy regulations. Global solutions are difficult because of varying viewpoints, philosophies, and technological needs. There are differences in opinion on internet usage and data protection, with some states calling for strict regulations (Turianskyi, 2020).

According to Świątkowska (2020), there is also a need to balance security with citizens' human rights, particularly privacy and freedom of expression. However, there are challenges when it comes to electronic monitoring. Such problems have been observed in Nigeria, where a proposed bill that would have fined and imprisoned people for making inappropriate and abusive comments on social media was removed in response to public protest of the bill. Furthermore, criticisms were levelled against a directive issued by the defense minister of Nigeria to keep an eye on social media accounts in order to stop the spread of hate speech (Ndubueze, 2020). It is important to emphasize that when implemented properly, security measures can significantly protect these rights, such as encryption and pseudonymization. Despite challenges, balancing security with human rights remains crucial (Świątkowska, 2020). Moreover, by working with technology specialists, policymakers can design appropriate laws and regulations that do not impede but promote innovation.

2.7.5 Underreporting Challenges

In South Africa, the Cybercrime Police Units struggle to initiate investigations into cybercrimes due to low visibility and non-reporting. In many cases, financial companies, especially, are unwilling to report cybercrimes due to reputational concerns. Some victims fear that reporting such cases may show them in a bad light, potentially negatively affecting their brand values, image, and reputation (Chudasama, Patel, Shah & Shaikh, 2020). They also believe they have better knowledge of the challenges and adequate resources to respond to them. (De Paoli, Johnstone, Coull, Ferguson, Sinclair, Tomkins, Brown, and Martin,2020).

Apparently, the police cannot play a key role in combating industrial misconduct without the active collaboration of the private sector and the companies involved (Gumbi, 2018). In some cases, victims do not report because of the fear of being blamed for these offences. Eoyang et al. (2018) argue that a blame-the-victim mentality has driven the American government's focus on defending systems and networks, with companies often blamed for breaches. They believe that companies should be held accountable for not addressing known vulnerabilities.

There are also challenges with the lack of knowledge. Lack of understanding of the risks of cyberspace tends to make many Internet users vulnerable to cybercrime. For instance, a victim of identity theft online might not be aware of the theft until the offender uses the stolen identity to carry out a criminal activity (Ndubueze, 2020). In other words, cybercrimes usually go unreported because some individuals may be unaware that they have been victimized, and they may also not want to recognize they are victims. They may view the offence as insignificant and need not be reported as it had a low impact. Moreover, they may be unaware or do not know how to report the crime (De Paoli et al, 2020 & Curtis & Oxburgh, 2022). Underreporting is also caused by issues of trust in the police department. There is a lack of confidence in the police (Chudasama et al., 2020). De Paoli et al., (2020) also report that the public may not report the crimes because they do not believe that the police can assist them in apprehending the offenders. Police also struggle to justify the impact on public interest, especially for low-impact crimes with one victim. Using the internet and ICT technologies allows offenders to generate revenue with minimal impact on one victim. The challenge lies in justifying public order breaches and initiating investigatory procedures. The need for new skills and policing concepts in cyberspace is paramount, and implementing these tools in practical environments remains the top priority (Chudasama et al, 2020).

Cybercrime incidents are also shockingly underreported because police officers lack the forensic technology expertise and competence to investigate cybercrimes. It is challenging for law enforcement officials to spot cybercrime patterns and trends due to underreporting (Ismail, 2020). Cases are left lacking even in cases where a complainant discloses a hacking or associated computer crime. Because of this, most laws and regulations must be passed to close this gap. Additionally, police officials must be educated, trained, and adequately equipped to handle cybercrime complaints. In the same vein, civil society participants must remain current

on developments in the cybercrime pandemic (Olofinbiyi, 2022).

2.7.6 Enforcement Gap Challenges

Baylon and Antwi-Boasiako, (2017) state that Cybercrime laws are frequently poorly enforced, even in cases where the laws are clearly defined. Prosecution also becomes more challenging due to the high number of victims who reside in other countries and not in the same country as offenders. Eoyang et al. (2018) assert that the absence of thorough public data makes assessing the cyber enforcement gap impossible. The possibility of apprehending a cybercriminal in the United States is less than 1% of the total number of harmful cyber events reported to the federal government each year, according to publicly accessible statistics from federal, state, and municipal sources. The fact that arrests do not always result in conviction suggests that this enforcement rate may be optimistic (Eoyang et al., 2018). Due to the absence of public databases providing enforcement metrics on computer crime across all localities, estimating an overall cyber enforcement rate can be difficult. This is evident in the United States when examining the difference in enforcement. Less than 1,000 people were arrested by federal, state, and local law enforcement authorities in 2016, despite the FBI receiving 298,728 reports about cybercrimes. An estimated 0.31% of enforcement actions and responses to cybercrimes are thought to be taken. Moreover, the number of convictions reported by law enforcement is lower than the number of arrests they made in 2016.

However, Eoyang (2018) argues that low enforcement rates are also influenced by the fact that victims hardly report cybercrimes. Discrepancies and inconsistencies were also discovered when almost two dozen databases were examined; none included complete attribution information. Lack of enforcement is also caused by the fact that Cybercrime investigation units are short-staffed and lack adequate training in VPN, darknets, and virtual currencies. Limited technical capabilities, outdated data/mobile forensics laboratories, malware forensics, and collaboration with local telecommunication service providers are also issues facing the governments. International cooperation, judicial cooperation, and relations with international service providers are also lacking (Van Vuuren, Leenen & Pieterse, 2020). Furthermore, police officers show an inability to adapt to changing settings. Police must change their organizational focus and take management's and line officers' opinions into consideration in order to strengthen cybercrime regulation.

Research indicates that officers, either as a result of a lack of organizational attention or a lack of confidence, do not think they should be the first point of contact for cybercrimes. Police focus more on traditional crimes than online crimes (Gumbi, 2018). Therefore, most cybercriminals practically go unpunished. This kind of crime is expanding, which makes sense given how simple it is to conduct these crimes and how improbable it is that they will be caught. Some researchers think the private sector ought to take matters into its own hands and launch an offence, considering law enforcement agencies' low response to these crimes. Victims will eventually decide not to report and/or take independent action if necessary (Eoyang, 2018).

2.7.7 Police Training and Education Challenges in Combating Cybercrimes

Education and training of the police are among the challenges facing law enforcement. Cybercrime and inappropriate online conduct are partly caused by the lack of expertise in developing nations, especially in the area of cybersecurity. With the 4IR development, the necessary skills are essential for digital security and safety. According to Świątkowska (2020) just 10,000 certified cybersecurity professionals are in Africa, despite the continent's 1.3 billion inhabitants. Of this number, 5,700 are in Sub-Saharan Africa, accounting for 4% of all ISACA-accredited specialists worldwide. Both formal and informal education are frequently inadequate. The educational system often lacks cybersecurity courses or research projects. This is especially difficult in less developed nations where knowledge of information security is not contingent on fluency in English (Świątkowska, 2020). Developing countries lack the specialized police and computer expertise required for effective law enforcement. According to a UNODC assessment, barely half of committed law enforcement officials receive regular training, and 70% lack computer skills and equipment. The majority of countries need technical support for cybercrime investigation methods. In the fight against cybercrime, unprepared prosecutors and court systems also provide a major obstacle (Świątkowska, 2020). Research conducted in England and Wales reveals that most people do not fully understand the dangers and threats of using digital devices. Nonetheless, victims believe that law enforcement is ill-prepared to handle cybercrime, and data has corroborated this claim, with 61% of officers classified as ill-prepared to deal with cybercrime (Curtis & Oxburgh, 2022).

Curtis and Oxburgh, (2022) further observe that another challenge is that Police officers often view cybercrime as different from traditional crimes, affecting their preparedness and

confidence in responding to such cases. Police are not adequately trained, and there's a propensity to think of cybercrimes as less severe than ordinary crimes (Nowacki & Willits, 2019). For instance, police officers might not consider cybercrimes as serious as traditional crimes because Cybercrimes are often not as visible, or their impact is often not as apparent. Therefore, police officers may not view responding to these crimes as real police work. They might also place the blame elsewhere, on the victims not being careful or other parts of the criminal justice system. For instance, Cyberbullying may be seen by Canadian police as a non-crime, and they may prefer education-based prevention (Nowacki & Willits 2019). The absence of suitably qualified personnel in many police organizations makes cybercrime training a major problem. Technological abilities are not given as much weight in the hiring process as physical attributes, critical thinking, psychological stability, and an impeccable track record. There is a conflict between the belief that all police officers should look into cybercrimes and that these investigations should be limited to fewer experts, as training may be shallow and ineffectual if all police are involved (Nowacki & Willits, 2019). Moreover, Governments are also concerned that cybersecurity skill development may cause dual usage. For instance, Cameroon is starting cybersecurity skill development programmes, but there are concerns that trainees could conduct cybercrime using the same skills (Orji, 2021).

Baylon and Antwi-Boasiako, (2017) assert that through training and capacity-building programmes, foreign governments and agencies have tried to combat cybercrime, but much of their efforts have been in vain. Specific programmes also focus on training particular groups, such as prosecutors, without offering detectives who investigate and send the cases to court for trial the necessary training. A better understanding, therefore, and appropriate training for police officers is crucial for responding to cybercrime cases. Officer training predicts an officer's preparedness to engage with victims (Curtis & Oxburgh, 2022). Cybercrime investigations involve gathering evidence, identifying suspects, examining crime scenes, and identifying evidence sources. However, the process is impeded by a lack of knowledge, anonymity of suspects, investigators' lack of understanding, and the asynchronous nature of the Internet. Law enforcement and policing organizations are ignorant about cybercrime, which is thought to play a significant role in the low conviction rates for cybercrimes (Curtis & Oxburgh, 2022). According to Świątkowska (2020), integrating cybersecurity into education is a critical first step toward government participation in the cyber field.

An educational framework can be established using international standards, rules, and courses specifically designed to improve the abilities of police officials to deal with cybercrimes. Non-governmental organizations ought to take part in these initiatives as well. According to Nowacki and Willits (2019) investigators who attend cybercrime-related courses treat cybercrimes more seriously and give these cases more of their attention. Because many cybercrimes occur across different geographic regions and the reacting unit may not always be clear, jurisdictional concerns often present a challenge. Victims' confusion about where to report an offence usually makes problems worse.

2.7.8 Cooperation and Collaboration Challenges

Responding to Cybercrime is also hindered by the increasing role of the private sector, which owns infrastructure, provides products and services, and maintains databases. The police are often unaware of service providers' developments and communication products. Law enforcement experts rely on cooperation with these organizations, often of foreign origin. Governments must establish efficient mechanisms for public-private cooperation through international initiatives. Public-private cooperation is crucial as new technologies and applications present more complex challenges (Świątkowska, 2020).

The Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in 2018, aims to solve data access issues across borders, requiring US-based tech companies to provide data to federal law enforcement, even if servers are located on foreign soil. Tech giants like Microsoft, Facebook, Apple, and Google supported the creation of the CLOUD Act. (Świątkowska, 2020). Limited collaboration between organizations such as ISPs, corporations, academic institutions, and governmental bodies exacerbates the problem of cybercrime. ISPs are required by the Electronic Transactions Act to assist law enforcement technically, although they hardly ever comply (Baylon & Antwi-Boasiako, 2017). Collaboration between public and private sector agencies to improve industrial espionage countermeasures is needed, with each entity providing a distinctive contribution to the effective implementation of the Act (Gumbi, 2018 & Dlamini & Mbambo, 2019).

2.7.9 Corruption Challenges

Cybercrime laws, policies, and infrastructures are ineffective in curbing the proliferation of cybercrimes against victims, institutions, individuals, and governments.

The human element, particularly corruption, weakens the security infrastructure (Richards & Eboibi, 2021 & Baylon & Antwi-Boasiako, 2017). Jason Jordaan, Head of the Cyber Forensic Laboratory of the Special Investigating Unit, South Africa, highlighted that corruption in organizations and institutions allows cybercriminals to perpetuate crimes, causing significant damage to victims and potentially perpetuating the crime from trusted domains: poverty, greed, and the desire for wealth drive insiders in Africa to assist in cybercrimes. Cybercrime institutions and stakeholders, including law enforcement agents, financial institutions, and postal agencies, are part of organized groups in Africa. Richards and Eboibi (2021) maintain that Cybercrime has persisted due to law enforcement authorities in Nigeria being corrupt, with certain police officers and EFCC staff acting as crucial informants. In exchange for payment, bank employees and postal workers assist offenders in the clearance of items and money. Because corrupt law enforcement officials are more interested in taking bribes and abusing innocent individuals, citizens cannot report cybercrimes. For example, con artists occasionally pay courts or police officers to ignore and disregard their actions or illegal acts (Baylon & Antwi-Boasiako, 2017).

Sub-Saharan Africa and Nigeria's security systems are rife with corruption. As a result, people would much rather look for other ways to fight cybercrimes than submit them to security authorities since they don't trust law enforcement to be honest and capable of stopping crimes. According to Richards and Eboibi (2021), Nigeria's Special Anti-Robbery Squad (SARS) is failing to curb cybercrimes due to corrupt practices. They use their power to arrest, investigate, and prosecute cybercriminals for personal gain, victimizing innocent people, unlawfully searching devices, and releasing them after collecting money. The Nigerian government's corruption and failure to eradicate criminal behavior contribute to the proliferation of cybercrimes (Richards & Eboibi, 2021). In Ghana, corruption has led to the proliferation of internet scams, with corrupt officials, police, and postal agents collaborating with cyber criminals. Police officers act as informants, relaying information to avoid prosecution, while immigration personnel provide resident permits for cybercriminals. Bank staff and money transfer agents help cybercriminals access proceeds, with fees for goods and money orders. Corruption contributes to the lack of enforcement and the cybercrime challenge, as fraudsters may bribe law enforcement or judges to overlook their activities. In South Africa, corruption-fuelled cybercrime has resulted in insiders giving cyber criminals access to critical information, bypassing security systems and making it harder to detect (Richards & Eboibi, 2021).

To discourage others and stop the spread of cybercrimes, law enforcement officials in the US have been proactive in their investigations and prosecutions of offenders. The United States of America v. Muhammad Fahd & Ghulam Jiwani case illustrates how hackers bought off insiders or workers of a business entity to help them carry out cybercrimes by infecting computers with malware, among other things. The defendants face 14 charges, including wire fraud, deliberate damage to a protected computer, accessing a protected computer to conduct fraud further, and conspiracy to commit wire fraud under the Computer Fraud and Abuse Act. (Richards & Eboibi, 2021).

2.7.10 Digital Expertise and Technology Innovation Challenges

Police and the criminal justice system face challenges from technological innovations, and Low-cost digital technologies are frequently blamed for cyber offenses. According to Johnson, Faulkner, Meredith, and Wilson (2020), Science and technology have a double edge, helping law enforcement with contemporary crime scene investigation, fingerprinting, forensic DNA analysis, and databases that allow for quick information exchange and, the other effect, helping cyber offenders. Cybercrimes are increasing; however, the expertise and resources needed to combat cybercrime are frequently beyond the capabilities of national law enforcement authorities. Using sophisticated digital tools or technology is part of cybercrime enforcement. However, there is very little digital policing in many African nations. Some states frequently use conventional techniques to look into cybercrime issues. Ismail (2020) states that certain countries were using digital technology inadequately and at a low level. They lack the necessary technologies, such as computer and internet systems, artificial intelligence (AI), tracking devices, integrated databases, surveillance software, and Internet of Things (IoTs), for combating cybercrime (Ismail, 2020). Świątkowska (2020) argues that the way the internet is designed to provide anonymity and the ability for criminals to operate behind several layers of false identities encourages covert activity by making it more challenging to identify the perpetrator. The digital environment poses difficulties for even the most fundamental processes, such as gathering, preserving, and assessing evidence.

Challenges associated with those procedures stem from the requirement for highly developed technological expertise and the reality that obtaining evidence will be impossible without

coordinated global efforts, sometimes including the private sector. Ismail (2020) states that Cybercrime detection, digital evidence seizure, investigation, and prosecution are high-skilled activities. Unlike a real crime scene, a digital one cannot be sealed with yellow tape. Therefore, delaying finding and confiscating evidence after a cybercrime has been committed may change the scene. In essence, it's critical that police investigators receive advanced training, develop their competence, and acquire more advanced technical knowledge and skills than cybercriminals. It can also be argued that some police officers are not computer literate and lack many IT specialists among cybercrime detectives (Ismail, 2020). Highly skilled law enforcement personnel are needed to deal with such crimes. The judicial system and law enforcement must continually invest in resources and develop strategies in order to keep up with the rapid growth of cybercrime tools brought about by technological improvements (Świątkowska, 2020).

Johnson et al. (2020) argue that the Police Service faces difficulties adjusting to scientific and technological advancements in crime and the criminal justice system. They lack resources, facility development, and technical expertise in law enforcement. This may be due to the lack of funds offered by the government to allow for more police training and proper development of effective mechanisms to ensure the fight against cybercrime does not lack (Johnson et al., 2020). Law enforcement, the judiciary, and government organizations are among the many institutions where cybercrime is becoming an increasing threat. For instance, according to Baylon & Antwi-Boasiako (2017), The Ghana Police Service's Commercial Crime Unit's Criminal Investigations Department lacks the technical skills required for digital forensics: the retrieval and examination of electronic evidence. There are limited sufficient computer labs for digital forensics within the police force. Furthermore, challenges come with a fear of training police and offering the skill and training because some officers leave the public sector for private employment after receiving the skills. The motivation to go to private companies is usually motivated by better or higher salaries (Baylon & Antwi-Boasiako, 2017).

2.7.11 Digital, Electronic Evidence, and Forensic Investigation Challenges

Large volumes of data may be stored on computers nowadays, which makes it challenging to freeze evidence. Accessing files may invalidate important evidence, and locating pertinent evidence among vast volumes of data might be difficult. Digital evidence can be stored on several servers thanks to modern distributed computer systems.

However, connecting to the Internet makes the issue more challenging since digital evidence can be dispersed over large geographic areas and legal jurisdictions. Testimony demonstrating that the evidence has been under the supervision of law enforcement officials and qualified investigators is necessary to guarantee the validity of fact. Written digital evidence must be verified and compliant with the Best Evidence Rule (Mugisha, 2019). Dlamini and Mbambo (2019) state that Initial errors, such as disregarding, discarding, or improperly managing digital evidence, are typically why computer-related investigations may fail. For countermeasures to be successful and cybercriminals to be apprehended, there should be as little delay as possible. When they do not have enough proof, law enforcement officers hesitate to take early action against hackers. Determining if the cyberattack is fraudulent and/or unlawful is crucial for a quick and efficient response. This guarantees that cybercrime will be addressed clearly and quickly (Dlamini & Mbambo, 2019).

During court procedures, the evidence's proponent does not have to call a coder to testify; instead, they should contact a witness who can explain how data is handled by the computer and utilized by the company. Most courts have used the business records exemption to address hearsay cases involving objections to adopting computer records. If audit logs meet the requirements, this method could be effective. However, it might not be appropriate for computer records to be gathered during an investigation as opposed to being the outcome of a regular, periodic procedure (Mugisha, 2019). Indeed, the field of digital forensics presents challenges. The instability of digital evidence is a significant problem since it requires much skill to obtain and maintain its integrity during legal proceedings (De Paoli, Johnstone, Coull, Ferguson, Sinclair, Tomkins, Brown, & Martin, 2020). Computers are integrated into more significant systems, enabling previously unattainable levels of information production, processing, and transmission as they get smaller, quicker, and less expensive. As a result, digital evidence appears in unanticipated locations and formats. Digital evidence is more challenging to gather and evaluate since places are instrumented for various uses, including interactive control of environmental monitoring (Mugisha, 2019). Banks, factories, retail inventory, hospitals, schools, companies, and government agencies are all managed by computerized control systems.

Computers and software programs are embedded in various vehicles, tools, equipment, machinery, telecommunications systems, and public switched networks.

Each of these sources is a potential source of digital evidence, but the collection, storage, analysis, and presentation are constrained by evolving legal standards (Mugisha, 2019). Wiretapping is one of the tools used to obtain electronic evidence; however, its invasion of privacy has caused issues and worries for the judicial system. This procedure is governed by the Pen/Trap legislation and the Wiretap Act. Like telephone wiretaps, law enforcement and private litigants are increasingly searching online for digital evidence as computerized technologies grow more widespread. Using bug-like devices or integrated communication technologies, including wiretap Trojans and packet sniffers, is known as wiretapping. In order to secure a wiretap court warrant, law enforcement must prove probable cause and have used all other less invasive options (Mugisha, 2019). Another challenge is that law enforcement professionals do not well understand several technical provisions of the current laws due to their technical character. Forensic knowledge is necessary for the search and seizure of digital evidence; this is a skill that is not as common among law enforcement officers (Ndubueze, 2020). In US 38.7% of law enforcement agencies lack the necessary personnel to handle cybercrime cases, and 23% cannot handle forensic and digital evidence. only 37.1% of police officers felt comfortable using computers and 35.3% had received training for dealing with online incidents (De Paoli et al., 2020).

2.7.12 Funding Challenges

Orji (2021) states that a shortage of qualified cybersecurity specialists that can help law enforcement agencies to prevent, investigate and prosecute cybercrime results from inadequate financing for cybersecurity programmes. Since cybersecurity is often not regarded as a national security priority, insufficient funding for cybersecurity activities in African governments is a major concern. This is related to issues of physical national security, such as terrorism, which are sometimes seen to be more widespread than cybersecurity problems. Cybercrime rates are also rising due to end users' ignorance of ICT applications and information society services. Many Africans are only now beginning to use the internet and lack the fundamental information needed to protect themselves from the risks associated with the internet. Governments need to invest more and provide more funds to deal with cybercrimes. Without proper and enough funding, Criminal law enforcement mechanisms may be unable to provide sufficient deterrence to cybercrime (Orji, 2021).

Moreover, more security measures are required to prevent cybercrime due to the growing and diverse threats to cybersecurity. If they have enough funds, businesses and organizations may install secure firewalls, conduct regular risk assessments, preserve digital evidence, identify content, detect intrusions, acquire cyber intelligence, and monitor their networks around the clock. Dlamini and Mbambo (2019) state that law enforcement also uses live connections from suspects to combat cybercrimes, and cyber forensic investigators can identify intrusions and counterattacks. But these operations are costly. According to UNODC studies, because these efforts are not adequately funded, the issues concerning cybercrimes become common factors across government agencies (Dlamini & Mbambo, 2019).

2.7.13 Lack of Knowledge and Awareness Challenges

One of the primary obstacles impeding the management of cybercrime is the general lack of knowledge of cyber security protocols and the potential for exploitation among internet users. Many nations still struggle to develop national cyber security awareness programs and successful cyber awareness campaigns (Ismail, 2020). Africa's lack of knowledge about cybercrime raises apprehensions about its potential to become a safe harbor. The lack of awareness also affects the judiciary's ability to manage cybercrime cases. Some cases may take longer than others, and technical cases may require more time for determination. As African economies increasingly rely on ICTs and broadband capacity, the impact of cybercrime on these economies is expected to rise (Ndubueze, 2020). They also don't work with Civil Society Organizations (CSOs) to inform and increase internet users' understanding of cyber threats. Many people are vulnerable to cybercrimes due to a lack of awareness of cyber-related hazards and risky behaviors. As a result, this could influence how law enforcement investigates cybercrimes (Ismail, 2020). Indeed, Ndubueze (2020) states that establishing cybercrime laws in African nations is hindered by a lack of knowledge regarding security risks associated with ICTs. The United Nations Commission for Africa has expressed dissatisfaction with stakeholders' lack of familiarity with these issues. It has highlighted the necessity for increased ICT-related security knowledge to effectively create and implement cybercrime laws, especially for professionals in the criminal justice system.

Compared to developed nations such as America, Australia, and China, cybercrime in Africa is receiving less attention.

Regional cybercrimes and criminality conferences, seminars, and discussions might create more awareness of the issue and emphasize the necessity of regional collaboration. Just 11 nations have ratified the 2014 African Union Convention on Cyber Security and Personal Data Protection, which impacts member states' ability to work together to create and implement anti-cybercrime laws throughout the continent (Ndubueze, 2020). Maluleke (2023) argues that a lack of knowledge and regulation around cyber security also draws attention to the fact that developing nations often lack basic computer skills. Further, it highlights the absence of an appropriate integrated framework for legal and regulatory issues (Maluleke, 2023). Even Lawmakers frequently lack knowledge of technology and the Internet, which results in laws about cybersecurity that are poorly drafted and impractical (Turianskyi, 2018).

According to Baylon & Antwi-Boasiako (2017), In Ghana, a growing number of PCs with internet connections make them easy targets for fraudsters. Because of a lack of user knowledge, many do not have antivirus software installed or do not patch regularly. Sluggish connection rates and bandwidth constraints further hamper installation. Many people use unlicensed software, which is not updated automatically with security fixes. The scenario is made more difficult by their low-income levels and inability to access antivirus software in their native tongue. The nation's expanding internet population seriously threatens the public (Baylon & Antwi- Boasiako, 2017). De Paoli et al. (2020) also state that the knowledge gap results from underutilizing cybercrime classifications and terminologies. These definitions support law enforcement agencies in identifying and classifying crimes, setting priorities for resource allocation, and assigning cases to investigators. Furthermore, authorities fail to recognize or require a formal procedure, which means that even when cybercrime is reported, it is frequently not recorded. (De Paoli et al, 2020).

2.7.14 Lack of Resources

Police organizations have found it difficult to adequately address the increased demands on their resources posed by the significant increase in the prevalence of cybercrime in recent years. In the UK, this trend of cyberspace has coincided with a post-policing environment that is becoming more resource constrained. Because of this issue, there is a growing demand for cyber training provided by police organizations to be as effective and efficient as possible in equipping police personnel with the knowledge and abilities necessary to deal with this modern criminal issue

(Cockcroft, Shan-A-Khuda, Schreuders, and Trevorrow, 2018). Reports from INTERPOL further show few resources and expertise for preventing, identifying, and conducting investigations on cyberattacks. There has been little success with initiatives aimed at increasing the capabilities of law enforcement authorities to deal with cybercrimes (Orji, 2021).

African nations have also been challenged for their poor response to cybercrime because of insufficient resources for their law enforcement agencies' infrastructure, intelligence, and employees. It is commonly believed that African nations are primarily focused on addressing urgent problems like poverty alleviation and conventional offenses like burglary, rape, and murder. The battle against cybercrime is not keeping up (Cordero & Thaw, 2020). Furthermore, Nowacki and Willits (2019) state that agencies might not have the resources to respond to cybercrimes, even in cases where definitions of cybercrimes are widely understood. Agencies may also lack the information technology specialists needed for a successful response. When victims of these crimes recognize this, they are then skeptical about reporting these offenses. This inversely causes a negative impact as governments see no need to devote many resources to respond to cybercrimes (Nowacki & Willits 2019). Eoyang et al. (2018) argue that there has been an increasing emphasis on going after cybercrime offenders through law enforcement operations and imposing various costs to change their conduct. One example is the number of actions against cyber offenders working for adversarial nation-states. However, as the enforcement rate demonstrates, these attempts are insufficient. They have also not been adequately resourced or given the political leadership required to be sufficient.

2.8 The Types of Cybercrimes

Law enforcement encounters several cybercrimes in their line of work. Hjertstedt (2019) states that Cybercrime happens in various ways and on different internet services. Any crime committed using online services can be regarded as cybercrime. Shola (2021) describes cybercrime as using computers and the internet to deceive individuals, groups, or organizations. All crimes perpetrated through the use of information technology and the Internet are collectively referred to as cybercrime. Although cybercrime is sometimes called electronic or digital technology crime to this day, there is no specific, precise, or combined definition for cybercrime (Hjertstedt, 2019).

However, researchers have been able to divide cybercrime into two broad categories. There is type I, which is more computer-focused, and type II, which is computer-assisted.

Cybercrimes of Type I:

Cybercrimes of type I are virtually and technical in nature. They are committed to utilizing computer- related and enabled technologies, and their successful execution principally depends on computer- related and enabled technologies (Gumbi, 2018). They include property cybercrimes, mostly involving financial fraud, such as identity theft and online fraud. Computer-focused attacks may steal personal data and perpetrate fraud by using crimeware or malicious software. To access programs and systems, valid identification and authentication are necessary for these attacks. Malware can also use stolen personal credentials to carry out illegal internet operations. These cybercrimes usually happen once or discreetly, and the advent of crimeware frequently makes them easier to commit. Phishing, data theft, and manipulation via viruses or hacking are a few examples of type I cybercrimes (Gumbi, 2018).

Cybercrimes of Type II:

The second category, Type II, is cybercrimes involving individuals, which can be considered more deceitful. These crimes are perpetrated utilizing computer-related and enabled platforms, yet their success depends on human vulnerability, sensitivity, and possible judgmental errors (Gumbi, 2018). They are computer-assisted or -facilitated, luring victims with the use of trustworthy, well-known tools like web browsers and email. They are interpersonal cybercrime, involving personal attacks and taunting of the reputation of a victim, such as cyberbullying, cyberstalking, child exploitation, extortion, and blackmail. The underlying crime or offense in Type II cybercrimes either predates the invention of computers or can be committed without them. However, Gumbi (2018) notes that it is unlikely always to be able to distinguish between the two categories of cybercrimes with precision. Not all cybercrimes fall neatly into Type I or Type II categories; instead, they represent opposite ends of a continuum (Gumbi 2018). In Africa, cyber offending involves mostly cyber fraud, while Western countries experience cyberstalking, illegal pornography, hacking, and more (Kritzinger & Von Solms, 2012). As Africa has seen growth in the use of wireless connectivity and technological devices, they have also become the easiest target for cybercriminals. This is also evident in that South Africa is ranked along with Western countries as having significant challenges with scams, phishing

attacks, and fraud. South Africa also experiences a considerable challenge with identity theft (Capazorio & Hollis, 2017).

2.8.1 The Most Common Types of Cybercrimes

Świątkowska (2020) states that Cybercrime is a significant issue causing losses in different countries. Various types of cybercrime contribute to these losses, but analyzing trends and factors can help understand the landscape. This objective focuses on cybercrime types with significant economic impact.

2.8.1.1 Identity Theft

Identity theft involves unlawfully attaining someone else's bank accounts or personal details, often fraudulently, to make unauthorized transactions or purchases (Joynt, 2023). the cyber offender would steal another individual's personal information (such as date of birth, house address, name, email, etc.) to apply for loans and create false social media accounts. The victim may become a defaulter, and their credit scores may be severely affected if the loan is not returned. Victims of Identity theft not only experience financial loss but may also become victims of sexual predators, which may damage one's reputation. The victim may also be wrongfully accused or arrested if their identity was stolen to commit fraudulent crimes. Cyber offenders may use stolen identities to open accounts, buy big tickets or items, and provide fake citizenship for foreigners. The crime can occur from either an alive or deceased individual. Social media identity theft is rising (Chudasama, Patel, Shah & Shaikh, 2020 & Sawaneh, 2020). Social engineering is one technique used to mislead victims. It entails tricking victims using communication tactics to get them to divulge confidential information or behave in the offenders' best interests. Phishing is an additional technique that involves the theft of personal identification to make electronic payments.

This is typically accomplished through phony emails or hypertext links to bogus websites. According to Hjertstedt (2019), many criminals steal BankIDs, which can lead to financial gain and access to private data. BankID-related identity crimes have the potential to yield substantial revenues from more minor offenses, which can then be utilized to fund other criminal activity. In South Africa, Any information about an identifiable, living, natural person is considered personal under section one of the Protection of Personal Information Act (POPIA). This includes

details about their name, gender, sexual orientation, education, medical history, biometric data, personal opinions, and any private or confidential correspondence they may have received. In South Africa, identity theft is a common cybercrime fueled by growing internet connectivity, corruption, and challenges in obtaining a conviction. The Act aims to protect people's personal information and privacy rights (Joynt, 2023). It is unclear, however, how the law should interpret these crimes and how governments and other authorities should respond to them. It is challenging to stop the rise in identity-related crimes due to the absence of standard definitions (Hjertstedt, 2019).

2.8.1.2 Phishing Attacks

Phishing is a tactic used by scammers to get your data. In this scam, cybercriminals pose as legitimate or well-known businesses to email you (Chudasama, Patel, Shah & Shaikh, 2020). Emails usually indicate or require an emergency response and may seem to be from trusted sources such as banks or e-commerce platforms (Joynt, 2023). These emails are sent to trick the individual and steal financial information such as credit cards, usernames, or passwords. Usually, these emails include an attachment or link. Clicking on such links will direct you to a fraudulent website. Your sensitive information, such as your card number, UPI code, and other bank credentials, will be requested from you by the phony website. Additionally, going on these URLs can launch a computer virus on your system (Chudasama, Patel, Shah, & Shaikh, 2020 & shola, 2021 & Nnaemeka, 2023).

Sawaneh (2020) states that Because phishing assaults are so successful, they happen often. Phishing schemes are the most common type of online fraud in South Africa. Many phishing e-mails appear to originate mainly in Ukraine, Ghana, Russia, and Nigeria. In Nigeria, phishing attacks are particularly committed by yayooh boys. Customers of several of Nigeria's major banks have fallen victim to phishing schemes (Ismail, 2020). In Ghana, phishing attacks are the second-largest category. Awoyemi, Omotayo, and Mpapalika (2021) explain that this cybercrime creates malicious modems by evading security mechanisms using wireless routers like WPA2. A variety of passwords may be accessed unlawfully using such techniques. In this case, end users can safeguard their accounts as a preventative step for regular internet users by regularly adjusting their privacy settings on networking sites following cyber security procedures.

Another crucial protective strategy is to ignore links that show up in questionable or suspicious emails. Using anti-virus software, firewalls, and anti-phishing toolbars are further measures to guard against phishing assaults. Further limit your online activity to secure websites with `https' in their URL (Awoyemi, Omotayo & Mpapalika, 2021). In order to deal with this crime, investigators use ethical hacking to check network system vulnerabilities and unsolicited emails from spammers. The recommended Multi-Split Spam Corpus Algorithm (MSSCA) identifies the spam thread that appears the most frequently in the email collection. However, Awoyemi, Omotayo, and Mpapalika (2021) noted that the financial industry is becoming concerned about the unauthorized usage of bank credit cards. As a response, banks in Nigeria decided to implement software that makes sure customer data is difficult to access. To combat fraudulent activities, commercial banks in Nigeria installed biometric identification systems in all states.

2.8.1.3 Malware and Ransomware

Ransomware is where a hacker encrypts data and restricts access (Kagita, Thilakarathne, Gadekallu, Maddikunta, & Singh 2020). After encrypting the victim's data, the hacker will require payment methods such as Bitcoin to release the system. It can have a major effect on a victim's finances and the country's economy. For instance, 300,000 people were impacted by WannaCry in May 2017, which forced computers running out-of-date Windows operating systems to shut down. The British National Health Service lost £92 million due to the disruption to the UK health system. The attack caused an estimated $4 billion in losses to the international economy. Attacks involving ransomware also severely damaged critical infrastructure (Świątkowska, 2020).

The term Malware is short for 'malicious software', and consists of computer viruses, worms, Trojan horses, ransomware, spyware, and all other types of destructive software or code. These impair or infiltrate a device or system without the user's knowledge to execute specific damage (Alexandrou, 2021). Malware and fraud are associated with data breaches that reveal that data was disclosed to an unauthorized person. Access to personal and corporate information is a primary goal of criminal activity. This may be done for extortion, cyberespionage, or financial gain via sales on the Darknet (Świątkowska, 2020). Malware such as Trojans, worms, and viruses are malware that pose as beneficial programmes or software. They can duplicate themselves and bind to other feasible programs; these viruses can reproduce throughout compromised systems

and lead to data loss. Resident, non-resident, boot sector, and macro viruses are the four categories of viruses (Alansari, Aljazzaf, & Sarfraz, 2019). A resident virus is implanted in the memory of a target system, which activates every time the system starts up or opens. Non-resident viruses do not remain in the system for long; they spread infection across network sites. The boot sector virus is aimed at hard disks. Whenever a compromised device is booted, the macro virus, loaded in the memory, launches automatically when a document is opened in Word, Excel, or Outlook (Alansari, Aljazzaf & Sarfraz, 2019). Malware is becoming a big issue in Africa. Africa reportedly has one of the highest rates of mobile malware infection worldwide, according to the 2017 Infocyte Report. The following IT infrastructure ratings for a few African nations are shown in the report: The Ivory Coast (81%), Kenya (78%), Senegal (78%), Tunisia (74%), Morocco (66%), Algeria (84%), Cameroun (82%), Nigeria (82%), Libya (98%), Zimbabwe (92%), and Mauritius (57%) (Ndubueze, 2019). Banking malware is an additional particular category of cyber threat. This threat has grown more serious due to the expansion of Internet banking. Banking Trojans software designed to get banking information illegally is becoming increasingly popular in this field. There is a suggestion that the growing usage of mobile banking apps is one of the leading causes. According to Check Point, a software supplier, there were 50% more attacks targeting mobile devices in the first half of 2019 than there was the year before (Świątkowska, 2020).

2.8.1.4 Fraud (Online Fraud, Online Shopping fraud, Advance fee scams and Credit Card Fraud)

- Online Fraud

The Swedish National Council for Crime Prevention reports an increase in fraud in today's society, primarily due to increased internet use and technical developments. Online fraud targets multiple people simultaneously, making it the most prevalent crime type (Hjertstedt, 2019). Online fraud entails tricking people into giving up crucial account information, stealing their money, espionage, or impersonation. The prevalence of this phenomenon has increased with the availability of banking and financial services on the Internet. Banks and information security firms have developed specialized technologies to safeguard clients and ensure the security of online transactions, while cybercriminals constantly devise new methods to deceive their targets.

Cybercriminals never stop innovating and looking for openings to complete their duties (Younes, 2019). Cybercriminals usually make fraudulent calls to potential victims using websites, chat rooms, email, Internet forums, and other web services. It frequently seeks to "embezzle" money, send checks or money transfers, or coerce people into disclosing personal information for espionage, impersonation, or access to confidential account data. There has been a massive increase in online fraud, with losses above $30 billion in 2014. Scammers use creative methods and adept imitation techniques to lure victims, preying on their greed, ambition, ignorance, and inexperience. Scammers typically use money transfers to steal money from victims, buy fake goods, or obtain personal information. They also take advantage of social media accounts by stealing and using them for advertising or private gain. Another strategy con artists employ to deceive people or gain services without payment is providing free access to services (Younes, 2019).

- Online Shopping Fraud:

Cybercriminals use fake internet shopping platforms to deceive their victims. These websites present appealing items at affordable costs, yet frequently, the goods are not delivered or delivered but not to the consumer's satisfaction. There is no customer service department and no return or refund policy. To counter this, a knowledge centre is often created, drawing students interested in professions such as law enforcement and cybercrime. For cybercrime complaints, law enforcement authorities ought to establish a centralized system for referral, and private companies may offer more excellent investigative knowledge (Chudasama, Patel, Shah & Shaikh, 2020).

- Credit Card fraud:

Credit Card fraud has increased in online transactions, the foundation of e-commerce business, and the overall expansion of digital commerce. The main goal is to obtain products without paying for them, make large transactions, and steal card information (Deora and Chudasama, 2021 & Sawaneh, 2020). Credit card scams happen when a customer conducts a fraudulent transaction since they don't need to physically show their card to the shop to purchase an item. The information required for these crimes are passwords, credit card numbers, and identities of the victims which can be obtained in various ways, such as phishing and data purchases on the dark web (Świątkowska, 2020).

2.8.1.5 Advance Fee Scams (or Fraud)

Online advance fee fraud is also a common challenge in Africa (Ndubueze, 2019). The majority of advance fee frauds target oblivious victims through emails. These emails are full of scams that seem to be from people giving away enormous sums of money to victims who just need to pay a little fee to have the money processed and sent to them. Phishing and advance fee schemes operate on the same fundamental principle. The email's format is the only thing that differs. Advance fee schemes use social engineering to trick victims into paying a modest deposit in exchange for a larger sum of money instead of pretending to be a trustworthy website to get their personal information. As a result, victims have to pay the criminal but never hear from them again after paying (Joynt, 2023).

2.8.1.6 Theft of the Intellectual Rights

Theft of copyrighted materials, such as trade secrets, trademarks, and other essential copyrighted items, is known as intellectual property theft. Copyright is the legal right granted to the publisher, storyteller, composer, artist, or musician who created the original work to reproduce it, usually for a restricted time (Sawaneh, 2020). Intellectual property theft occurs when individuals violate copyrights or download unlicensed intellectual property online (Shola, 2021). Copyrighted content, including images, designs, and trade secrets, is frequently stolen from other people. Copying software or movies on digital video discs (DVDs) from any international companies and selling them to the people at the lowest cost, decoding private satellite channels, which are encrypted and have subscription fees. (Alansari, Aljazzaf, & Sarfraz, 2019). Younes (2019) further states that young people are frequently drawn to these things and work in upmarket companies that offer generous benefits and high incomes. Moreover, Cybercriminals also deceive these young people into accepting outrageous employment offers, which could result in money or personal information being stolen. Individuals could get notifications that they have won something (such as a lottery), but they must transmit their identity cards or data. In order to obtain information, some scammers construct fake websites. These pages frequently present innocent scenarios or issues, like an email threatening to cancel an account if it isn't activated within a day. People often click the link to the fake page quickly and fall victim to cybercrimes (Younes, 2019).

2.8.1.7 Spamming

Spamming is the practice of sending unwanted mass messages or emails randomly using electronic messaging networks (Ismail, 2020). The unwanted emails are sent online for phishing, virus distribution, and advertising. Spams may come as instant messaging services, Usenet newsgroups, blogs, wikis, online classified advertisements, internet forums, social networking sites, and online classified ads. The ease of access for spammers has led to a rise in spam emails. Spams in 2011 incurred around $7 trillion in costs for users and internet service providers. Different countries have different policies regarding spam. For instance, the Electronic Communications and Transactions Act in South Africa mandates that anyone sending consumers unsolicited commercial communications, referred to as spam, must give them the option to unsubscribe from the mailing list (Alansari, Aljazzaf & Sarfraz, 2019). Microsoft often assists law enforcement officers in Nigeria by giving leads on spam coming from Nigeria, enabling the government to launch investigations more quickly and effectively. Spam in Nigerian e-banking is alarming (Ismail, 2020).

2.8.1.8 Cyberstalking/Cyberdefamation

Cyberstalking is the act of disrupting someone who is online in order to commit a crime. Examples of this behavior include messages placed on a website, social media group messaging applications, email, and instant messaging (IM) (Nnaemeka, 2023 & Sawaneh, 2020). The attacker uses malicious software to conceal their internet identity so they may harm the victim without being discovered (Sawaneh, 2020). The perpetrator may use an email to track out a victim, typically a female or child, by threatening them, using abusive language, or making strange requests. In Nigeria, one of the most common forms of cybercrime has been found to be cyberstalking (Ismail, 2020). Cyberstalkers may also deliberately violate an individual's online reputation. Accounts of victims may be hacked, and they may be harassed or bullied, which can result in trauma, drug addiction, financial loss, and emotional abuse. They create false accusations, identity theft, data theft, and the use of child pornography (Shola, 2021 & Ndubueze, 2019). A Cyber stalker could be a stranger or a person wanting vengeance or is angry (Deora & Chudasama, 2021).

2.8.1.9 Hacking

Hacking is the process of gaining unauthorized access, interfering with, or intercepting data by using “smart” network techniques. Hacking can be described in a similar classical crime scenario to its best practice. Similar to housebreaking, hacking involves using cunning methods to enter a location where entrance is prohibited. Breaking into a residence can lead to several consequences, such as property damage, theft, or extortion. The same is true for hacking and the consequences that arise from it (Joynt, 2023).

Deora and Chudasama (2021) mention three types of hackers: the white-hat hackers, who are ethical hackers employed by a company under contract to investigate computer system vulnerabilities; second is the grey-hat hackers, who strive to strengthen system and network security; and black-hat hackers, who operate unlawfully. Blue-hat hackers breach networks without permission in order to reveal security holes to their owners. They are not affiliated with computer security consulting companies. Additional types of hackers include Script Kiddies, Phreakers, Hacktivists, and Elite Hackers. Saweneh (2020) states that unauthorized access to and password cracking of a computer system are done with the intent to examine, copy, or produce data. Regretfully, no system can completely protect itself from security risks. Humans live in a globally interconnected cyber world with devices connected by the internet. Some internet users, unaware that they and cybercriminals share the same source, make it simple for hackers to access their computers. Hackers, sometimes called crackers, gain access to computer systems through technical know-how and proficiency, which may lead to identity theft and significant financial damage. They utilize harmful malware to obtain more by stealing sensitive data and passwords or taking advantage of victims (Sawaneh, 2020). Hacking also involves stealing electronic information from banks, transferring money to a third-party account, and buying expensive items in the victim's name (Shola, 2021).

2.8.1.10 Cyber Vandalism

Vandalism is the deliberate act of causing harm or destruction to another person's property, while cyber vandalism is the act of causing harm or destruction to data on a network when it is interrupted or stopped. It might include any physical harm done to a person's computer or cloud server. Stealing a computer, a component of a computer, or a computer accessory are examples of such crimes. A cybercriminal may add, change, or remove content from someone else's website with harmful intent (Nnaemeka, 2023 & Sawaneh, 2020).

2.8.1.11 Cyber Extortion

Cyber extortion results from persistent denial of service assaults and/or other attacks by malicious cyber criminals on a website, email server, or computer device. It involves the stealing of confidential data and the threat of exposing it to the public in return for money to avert or terminate the attack. It is comparable to ransomware attacks in which cybercriminals demand money in exchange for a promise to either stop the assault or to offer protection (Nnaemeka, 2023 & Sawaneh, 2020)

2.8.1.12 Cyber Bullying

The increased use of social media by people of all ages and genders raises the possibility of undesirable behaviors like bullying, which can negatively impact a person's personality and inflict emotional and mental trauma. Cybercrime, which includes identity theft, credit card fraud, bullying, stalking, and psychological manipulation, is known as cyberbullying. A bully may intimidate, threaten or insult a victim. Naturally, sociable women are most vulnerable to cybercrimes after children, as they easily connect with virtual friends or online groups for discussions on cooking techniques, children, family issues, and post-pregnancy 'tips' (Al-Khater, Al-Maadeed, Ahmed, Sadiq & Khan, 2020). Cyberbullying victims may suffer from low self-esteem, anxiety, panic attacks, despair, insomnia, and antisocial conduct (Awoyemi, Omotayo & Mpapalika, 2021).

2.8.1.13 Cyber Terrorism/Cyberwarfare

Cyberterrorism involves large-scale disruption of computer networks for political or ideological reasons (Shola, 2021). Cyberterrorism is defined as any illegal act of violence against individuals, citizens, companies, or property, frequently motivated by racial, political, or ideological reasons. It ruins property, promotes violence, anxiety, and terror, and compromises the integrity and accessibility of knowledge. The internet is used by terrorists for public opinion, recruiting, propaganda, and infrastructure destruction. One such instance is the December 2015 attack on a power system by the Ukrainians. Cyberterrorism may lead to violence, fear, and disruption, which can affect political decision-making and result in significant economic loss, property damage, and possibly even fatalities as well as disrupt community cohesiveness (Al-Khater, Al-Maadeed, Ahmed, Sadiq & Khan, 2020).

2.8.1.14 Child Pornography

Images, movies, and audio recordings of minors in an inappropriate manner of clothes, positions, especially sexual positions, are known as child pornography (Al-Khater, Al-Maadeed, Ahmed, Sadiq & Khan, 2020 & Shola, 2021). According to Alansari, Aljazzaf, and Sarfraz (2019), Sexual e-crimes typically entail the use of stored data by offenders to create and distribute harmful content online or offline. These crimes can include extortion, in which a perpetrator may hack a computer to steal images and blackmail a minor through any recorded call. They may use flattering, in which young men take advantage of relationships by chatting with minors and developing trust in order to build a relationship with them, and corrupting young minds through sending pornographic images and videos (Alansari, Aljazzaf, & Sarfraz, 2019).

Abuse of children can happen in some places, such as households, communities, schools, or organizations. The worst sexual e-crime in US history was discovered in 2010 when 52 members of the worldwide pedophile child pornography group were found guilty of dispersing up to 16,000 DVDs of child pornography. In many nations, the use of child pornography is illegal and subject to penalties. Since laws don't keep up with the rapid advancement of technology, crimes committed on social media are frequently punished by applying current laws. Numerous investigations have been carried out about the possible impact of juvenile exposure to internet pornography, given the elevated frequency of exposure and the increased susceptibilities of young people to depression, interpersonal victimization, and criminal tendencies (Sawaneh, 2020). While studies try to lower the number of incidents, child pornography is disseminated for both commercial and non-commercial uses. The creation, acquisition, or dissemination of digital information, including child pornography, is deemed by the law to be a serious offense that impacts an individual's self-esteem, confidence, and sexual maturation. This act has serious psychological repercussions that may affect a child as well, leaving them open to sexual predators using the internet to target minors (Al-Khater, Al-Maadeed, Ahmed, Sadiq & Khan, 2020). A multifaceted strategy is required to address child pornography, including educating victims about social media safety, increasing public awareness of sexual misbehaviors, and enhancing digitally enabled techniques for tracking child pornographers online (Awoyemi, Omotayo & Mpapalika, 2021).

2.8.1.15 Denial of Service Attacks (DoS)

A cybercriminal's attempt to stop a system or network from providing its services so legitimate operators cannot use it is known as a denial-of-service (DoS) attack. Another type of DoS is distributed denial- of-service (DDoS). These attacks overload servers with requests, making it more difficult for the server to handle all legitimate requests. Attackers use a huge number of botnets to target services, flooding them with thousands of requests until they collapse and become unavailable (Kagita, Thilakarathne, Gadekallu, Maddikunta & Singh ,2020). While widespread DoS attacks need cooperation from several computer users, single DoS assaults are easy to handle. Botnets, networks of compromised computers, and malevolent internet users attach malicious software to well-known web servers, websites, or services to launch denial-of-service assaults that allow third parties to take over the system (Sawaneh, 2020). These attacks can occur through various methods, such as ICMP flood attack or Smurf attack, where A connectionless protocol called ICMP is used to find problems and troubleshoot networks. A target server experiences a server overload and crash due to an attacker flooding it with ICMP packets. SYN flood attack stops the target system from responding to authorized users; the attacker floods it with a number of SYN assaults. Teardrop attack manipulates fragmented and overlapped packets; the attacker overwhelms the target system and tries to put them back together (Al-Khater, Al-Maadeed, Ahmed, Sadiq & Khan, 2020)

DDOS attacks can be prevented or mitigated by implementing DDOS attack prevention services and increasing the traffic bandwidth of a company's website. Futuristic cyber-attacks can target new technologies and devices, such as Wi-Fi, healthcare devices, robots, and drones, which are highly vulnerable to cyber-attacks. Attacks that could affect Wi-Fi users include man-in-the-middle, key reinstallation attacks (KRACK), and signal jamming attacks (Al-Khater et al., 2020).

2.8.1.16 Cyber Espionage

Cyber espionage is any activity involving the illegal use of computers to spy and steal crucial and private data for the benefit of competing businesses or foreign governments. They can invade and monitor messages, emails, etc (Al-Khater, Al-Maadeed, Ahmed, Sadiq & Khan, 2020 & Deora & Chudasama, 2021 & Shola, 2021). However, cyber espionage is more acceptable than cyberattacks. This notwithstanding, cyber espionage raises legal and ethical concerns that are covered under international law and treaties like the Budapest Convention.

The United States supports creating new cyber espionage standards that permit countries to use cyber espionage for conventional intelligence gathering and to carry out vital national security operations (Sawaneh, 2020).

2.9 Recommendations on Approaches that Law Enforcement Can Adopt to Curb Cybercrime

Researchers have suggested several strategies that can assist in decreasing the risk of cybercrime in Africa and across all nations. Cybercrimes cross geographical boundaries and provide special difficulties for law enforcement organizations in prosecuting criminals and expanding the "pool "of potential victims. The worldwide scope of cybercrime leads to uncertainty among and within law enforcement authorities, especially in African nations. It is challenging for law enforcement to react efficiently to demands for service regarding cybercrime because they have challenges obtaining the technology, training, and retention of officers with the essential abilities to combat cybercrime (Koziarski & Lee 2019). There are also challenges to finding reliable information on cybercrime, and it is expensive to create and maintain security and preventative measures. Global financial institutions are frequently the focus of computer fraud and theft (Maluleke, 2023). The approaches and recommendations are suggested for combating cybercrimes.

2.9.1 Training and Capacity Building Programmes

Eoyang, Peters, Mehta, and Gaskew (2018) state that to deal with cybercrimes, there is a need to tackle the training, incentives, and retention of the cyber enforcement workforce. The judiciary and legal community must strengthen their ability to combat cybercrime, particularly the analysis of digital evidence. This is essential to the cybercrime strategy because it addresses needs, encourages collaboration, and advances. It is also important for judges, prosecutors, and law enforcement officials to have extensive training in managing electronic evidence (Van Vuuren, Leenen, & Pieterse, 2020).

Law Enforcement Officials Training:

Law enforcement agencies, the police, prosecutors, judges etc. are very concerned about the increase in cybercrimes, and to respond to these challenges, the police especially, frequently

set up specialist sections to combat cybercrime (Van Vuuren, Leenen & Pieterse, 2020). Gumbi (2018), however, argues that specialized techniques and procedures are not always readily available nor advanced enough to deal with the major increase in the types of cybercrimes that law enforcement officials encounter. Thus, law enforcement officials, legal practitioners, and presiding officers should be regularly and consistently provided with training in investigating and prosecuting cybercrimes (Gumbi, 2018). Training programmes must be focused on digital forensics strategies. First responders to cybercrime attacks, investigators, and supervisors are just a few of the jobs that should be covered in a training programme. To provide practical training in cyber security, African regions should create an academy that specifically deals with digital or cyber investigation training. The already-existing law enforcement training resources, and programmes should be effectively utilized and modified where necessary to incorporate reporting and investigation of cybercrime protocols (Van Vuuren, Leenen & Pieterse, 2020). The role of law enforcement must further be expanded to support capacity development initiatives in order to allow law enforcement to target offenders responsible for cyberattacks with diplomacy (Eoyang, Peters, Mehta & Gaskew, 2018).

Baylon and Antwi-Boasiako (2016) further state that since young people often commit cyber-criminal activities, development programs focused on youth are a necessity. Furthermore, the fact that many online offenders can commit these complicated types of offences shows they have technical skills. This implies that recruiting and training young people as cyber law enforcement officials to deal with such offenders could pay dividends. As an extension, programs could provide the youth with specific technical training to work for law enforcement agencies, and the public and private sectors in various online roles to combat cybercrime (Baylon & Antwi-Boasiako, 2016).

Judicial Training:

Specialized prosecution services are uncommon in the judiciary. Judges and prosecutors need to have some fundamental expertise to deal with cybercrime and electronic evidence. It is, therefore, essential to train attorneys, solicitors, and advocates, particularly in common law jurisdictions. To ensure sustainability, judiciary training needs to be included in the standard judicial training system. This includes creating training materials, developing trainers, and mainstreaming modules into the curriculum (Van Vuuren, Leenen & Pieterse, 2020).

2.9.2 Cybercrime Assessments and Evaluations

Cybercrime monitoring and evaluation are essential and may be conducted occasionally. It will not only help to assess law enforcement agencies' performance but also identify the gaps and weaknesses of the cybersecurity system. This kind of exercise will help develop capability and is also helpful in assessing the degree of cooperation and information exchange between various law enforcement agencies on a national and international scale. To raise Africa's level of cybercrime capacity, these exercises in its member nations are important (Van Vuuren, Leenen & Pieterse, 2020). Furthermore, Periodic evaluations of laws are required to capture shifting cybercrime patterns and enhance cybercrime legislation and policing throughout Africa (Ndubueze, 2020).

2.9.3 Improved and Updated Cybercrime Laws/Legislation

Cybercrime trends are ever-changing; therefore, a constant review of cybercrime-related laws is needed to address cybersecurity hazards effectively. An institutional framework must be developed to monitor the information security system, keep up to date with the latest information security, and manage information security risks such as information reporting, security breaches, and incidents. Governments need to create, oversee, execute, and approve policies and strategies that are cohesive and work in accordance with one another (Van Vuuren, Leenen & Pieterse, 2020). To prevent, identify, and punish cybercrime offenders, countries must build strong legal frameworks that facilitate the implementation of new legislation and provide legal professionals with the skills to manage digital evidence. This involves classifying computer data and systems violations, such as unauthorized access, interception, and device misuse, as unlawful. Electronic evidence in criminal processes, accelerated data preservation, production orders, search and seizure of stored data, real-time traffic data collection, and content data interception for investigative purposes must all be addressed (Van Vuuren, Leenen & Pieterse, 2020).

Furthermore, many African countries have not signed the Convention on Cyber Security and Personal Data Protection document; therefore, the African Union (AU) should concentrate on persuading its member states to sign and ratify. Legislators may become national legislation advocates by using the Pan-African Parliament as a productive platform for convention

discussions. To create new policies, the AU should work with other stakeholders, including civil society, technological specialists, and European partners. African individuals should be involved in establishing laws, and governments should ensure that human rights and the rule of law are included in all domestic laws (Turainskyi, 2020).

The AU could consider creating a continental body similar to the European Network and Information Security Agency (ENISA) and applying the World Economic Forum's 'A Call for Agile Governance Principles' in future technology legislation (Turainskyi, 2020). Maluleke (2023) states that the quick evolution of techniques and improvements in ICT provide issues for South Africa when it comes to developing and implementing cybercrime regulations. Outdated regulations, inadequate training, and the frequent non-participation of government agencies hinder effective policing. The public, business, and academic sectors are working together more often, but more has to be done to increase cybersecurity awareness and enhance cybercrime policing (Maluleke, 2023). To convey a message to hackers and discourage future ones, it is imperative to implement current laws strictly. Regulatory bodies must step up their public education efforts, encouraging knowledge in the primary languages of the area and enhancing reporting procedures (Ndubueze, 2020).

Information and communications technology is becoming needed in the digital era, but it also risks our safety. The government should regularly conduct cybersecurity research, minimally control internet assessments, implement cybersecurity education in schools, and discourage the public from protecting or hiding cybercrime offenders to ensure a digitally safe online environment. Cybercrimes should have harsher penalties, and informants should be sent to various industries to monitor and report on hostile activity. To combat cybercrime, a robust plan that includes a fully financed research lab, professional skills, and cutting-edge technology should be implemented (Nnaemeka, 2023).

2.9.4 Collaboration and Cooperation on Cyber-Security Strategies

A more effective measure would require various stakeholders to become involved in tackling cybercrime, including prosecutors and the judiciary, private agencies, service providers, the technological sector, the government, and parliament.

What could be more effective is if the private investigation sectors or companies work closely with law enforcement (Hjertstedt, 2019). National governments must work together as it is a Global issue. Cross-border searches, seizures, extradition of cyber criminals, and the exchange of investigation leads should all be permitted under regional regulations (Ndubueze, 2020). Improved information sharing and collaboration between the public and commercial sectors (Such as ISPs, CSIRTs, RISK teams in the financial industry, and non-governmental organizations) are essential for preventing and managing cybercrime.

Countries may hold regional and international conferences that unite stakeholders to deliberate on the challenges. It may further provide beneficial networking opportunities and avoid delays in obtaining electronic evidence within and across international borders to accomplish prosecutions (Van Vuuren, Leenen & Pieterse, 2020). Global collaboration and cooperation are needed to conduct cybercrime investigations across borders effectively. A legal basis for international cooperation is provided by the Budapest Convention on Cybercrime, which mandates data preservation procedures and reciprocal legal aid. In order to promote tighter collaboration and the sharing of knowledge, ENISA and Europol have inked a strategic cooperation agreement inside the European Union. Furthermore, cooperation between internet service providers and police must be mandatory to improve efficiency. Argues that national legal frameworks alone may not be sufficient to deal with cybercrime. The regional and international police agencies must work to raise more awareness of new cybercrime trends and foreign measures of the criminal justice system (Hjertstedt, 2019 & Van Vuuren, Leenen & Pieterse, 2020). Moreover, African nations that have not yet ratified the Convention on Cybersecurity and Data Protection of the African Union must engage with the document (Ndubueze, 2020).

2.9.5 Funding Opportunities

More funding is also needed to develop forensic science technology, tools, equipment, and training programs. The government must Invest more in digital forensics and attribution technology research and development (Eoyang, Peters, Mehta & Gaskew, 2018). To provide accurate statistics and data that may direct the revision of cybercrime laws in African countries, the creation of specialized cybercrime research institutes is needed, and financing for such studies is required. The government must give the Cyber Intelligence Division (CID) more funding and prioritize combating cybercrime.

This will guarantee a deliberate, well-focused, and successful battle against cybercriminals and assist in addressing the increasing sophistication of cybercrime (Ndubueze, 2020). It will further provide Clear, detailed documentation on the best practices and provision of more resources, methods, and/or laws on handling cyber-based evidence. Statistics and data on how much money businesses lose to cybercrime must also be calculated. One way to measure the influence of cybercrime on the economy would be to conduct an economic analysis. This will assist in measuring its trends and how much resources and funding are needed (Baylon & Antwi-Boasiako, 2017).

2.9.6 Awareness and Educational Programmes on Cybercrimes

Law enforcement organizations employ technology to solve computer system vulnerabilities and improve consumer awareness to prevent online crimes such as identity-related crimes (Hjertstedt, 2019). To stop cybercrime, public awareness, and education are essential. It is important to create educational initiatives to increase public knowledge of cybercrime concerns. Public websites, instructional materials, and resources tailored to certain industries and groups can all be used as a form of support. To promote safe online conduct, best practices for cybercrime should be created. This includes making low-cost tools for spotting online risks. Encouraging children to use the internet appropriately, protecting their security and dignity, and avoiding sexual abuse and exploitation should be the main priorities (Van Vuuren, Leenen & Pieterse, 2020). Using an African Cyber Security Knowledge Framework, South Africa should cooperate with businesses, governments, and society groups to raise knowledge of cyber security. In order to create national education programmes for cybersecurity standards and research, the government should collaborate with institutions to provide professional training courses. It is advised to conduct yearly evaluations, simulated cyberattack tests, and regular national cyber security awareness campaigns (Gumbi, 2018).

For underdeveloped nations, creating cybersecurity courses built on internationally accepted norms would be a great way to start. Such initiatives should have the active support of the international community, particularly Western countries. However, the programmes should be customized to local settings and cultural environments. For instance, African countries have the least average access to higher education. Therefore, cybersecurity programs should be focused on the primary and secondary school levels (Świątkowska, 2020).

It is also important for decision-makers to consider socially vulnerable subpopulation groups such as women and the elderly in the implementation of focused initiatives. This will be in accordance with the precepts of Sustainable Development Goals and national values, as enshrined in the Constitution. Although developing nations can have limited resources, technology can assist by providing free online learning opportunities, high-quality education, and non-formal learning opportunities. With financial incentives from governments, private enterprises may also assist in providing cybersecurity training. Although these other channels (such as private companies) could aid in the dissemination of cybersecurity information, formal instructional programmes will still be essential for the general public (Świątkowska, 2020).

2.9.7 Cybercrime Reporting and Intelligence

For African countries to prevent and combat cybercrime, intelligence on possible risks is essential. Information from the general public, companies, and government organizations must be gathered and shared in order to assess and forecast trends. Having access to information concerning cybercrime is crucial to getting political support and funding. Creating avenues for users, persons, and organizations to report crimes can lead to law enforcement inquiries, offer intelligence regarding the extent, risks, and patterns of cybercrime, and facilitate the gathering of data to identify patterns of organized crime (Van Vuuren, Leenen & Pieterse, 2020).

2.9.8 Innovations and new technologies to strengthen Cybersecurity

To make the fight against cybercrime more successful, digital reality encourages innovative approaches aimed at urgent issues. Cybercrime serves as a catalyst for a sophisticated criminal ecosystem that includes Information Sharing, Coordination Centres, and organized criminal organizations. For individuals with minimal means, breaking essential links in the cybercrime economy can be profitable. The execution of specifically designed and targeted countermeasures might result from identifying crucial elements within cybercrime chains (Chudasama, Patel, Shah & Shaikh, 2020). The police or government can use AI, blockchain, and Machine learning to safeguard the public and lower crime rates by incorporating these technologies with policies in place. Because AI can quickly and efficiently analyze vulnerabilities millions of times, it can be an effective defense against hackers. It can identify frauds, scan emails before they are clicked, and prevent defects before an attacker can take advantage of them (Chudasama, Patel, Shah & Shaikh, 2020).

I. Blockchain:

Technologies currently in use and being developed, such as blockchain-based digital assets (BDA), can be used to locate key cybercrime ecosystems. Because of its capacity to handle massive volumes of data, analyze nonlinear datasets, identify or predict crime patterns, and connect seemingly unrelated pieces of information. The BDA quickly replaces traditional methods of fighting financial crime (Chudasama, Patel, Shah & Shaikh, 2020). It helps identify novel forms of payment fraud, particularly those combining cryptocurrencies and blockchain technology. Their coordinated implementation increases the efficiency of BDA tools through the use of international forums and cooperation initiatives. The effectiveness of BDAs and other cybersecurity measures, such as multimedia analytics and predictive policing, can be improved by Artificial Intelligence (AI) and Machine learning. AI and ML can detect and prevent spam, find security holes and provide solutions, forecast malware and new threats, and use behavior analytics to detect insider risks (Chudasama, Patel, Shah & Shaikh, 2020).

Nnaemeka (2023) explains that because BDA is decentralized, there is less chance of breaches and illegal alterations, and data integrity and safety are guaranteed. Blockchain removes the need for centralized sources by enabling safe digital identities. Because of its smart features, transactions are safe and automated, which lowers the risk of fraud and maintains transaction integrity. Additionally, blockchain reduces tampering, illicit modifications, and counterfeit objects by offering an auditable record of transactions. Organizations may better detect, prevent, and respond to cyberattacks by using blockchain, artificial intelligence, and machine learning technologies, creating a safer online environment (Nnaemeka, 2023).

II. Artificial Intelligence (Al):

Al has the potential to improve digital security through real-time analysis of massive data sets, trend detection, and identifying patterns. By examining user behavior, system logs, and network traffic, it is able to identify and stop attacks. AI-driven threat intelligence systems are able to detect or monitor international threats and detect new risks so that preventative measures may be taken. Furthermore, by employing behavioral biometrics, voice and face recognition, and fingerprinting to identify and stop unauthorized access attempts, AI can enhance user authentication and access control while lowering the risk of identity theft and account breaches (Nnaemeka, 2023 & Chudasama, Patel, Shah & Shaikh, 2020, Kazaure, Jantan, Yusoff, 2023).

III. Machine Learning:

Machine learning algorithms learn from historical data and adjust to new risks. They are able to identify abnormalities and malware and anticipate future threats. They activate early warning systems, identify malware based on network traffic, system performance, or source code, and predict future threats by examining historical attack data, user behavior, and vulnerabilities in the system (Nnaemeka, 2023 & Kazaure, Jantan, Yusoff, 2023).

2.10 CONCLUSION

It is evident that the increase in technological development has brought major challenges to society. Although technology is meant to bring about socio-economic development, it has also allowed many people the opportunity to engage in crime. Technology constantly evolves, and criminals become more skilled and find more ways to commit crimes. It is, therefore, important to keep up to date with what is new and emerging in cyberspace. Many countries have developed laws and formed collaborations to respond to cybercrimes. The African Union (AU) Convention on Cybersecurity and Personal Data Protection is one of the structures designed to respond to cybercrimes and offer international collaboration. It was established to address digital gaps and develop a legal framework for cyber-security and personal data protection. However, only a few countries have enacted national cybercrime laws, while others have drafted bills. Senegal, Ghana, Mauritius, and Morocco have ratified the Convention on Cybercrime and South Africa has signed the convention. More African states, however, still need to engage in the convention and provide cyber legislation to protect citizens, abide by the rule of law, and respect human rights. However, challenges persist in the wording of cybersecurity laws and the shift towards political stances.

Another international convention is the Council of European Convention on Cybercrime (CECC). The CECC has been working since 1976, providing guidelines and regulations for states and implementing international cooperation for cybercrime investigations and prosecution. As of September 2019, 65 countries have signed the Convention, defining conduct that national legislative initiatives should proscribe. The ECC includes countries across the globe, both African and Western countries. Forensic science and investigations are also developed and implemented to combat cybercrimes. Not only is digital valuable forensics in commercial, private, or institutional organizations, but it is also essential for law enforcement

and investigations. There are new developments in the AL, ML, and blockchain, as well as advanced technology to mitigate cybercrimes. The development of these new technologies has improved cybersecurity by enabling security professionals to immediately identify and respond to possible threats by finding patterns and abnormalities in network data. However, law enforcement requires highly skilled personnel and a constant review of laws and regulations to respond to cybercrimes effectively. Research shows that cyber law enforcement agencies face several challenges, including inadequate skills and knowledge, equipment, infrastructure and funding to fight cybercrime. Digital forensic experts are particularly crucial for the successful prosecution of criminals. The paucity of skilled human resources makes collaboration with other agencies like the FBI, Interpol, and Europol imperative.

CHAPTER THREE

THEORETICAL FRAMEWORK

3.1 Introduction

A theoretical framework is a structure a researcher uses to support a study or theory of research work. It stands to elucidate why the problem under study exists. Furthermore, a theoretical framework is a basis for conducting research; it directs and guides the study (Olayemi, 2014). With reference to the aims, objectives, and nature of the study, the researcher employed the Routine Activities Theory (RAT) and Structural Functionalism Theory to understand crime and crime prevention in cyberspace. These theories bring rich scholarly arguments on who, how, and why there are challenges in responding to or combating cybercrimes. These theories examine cybercrimes from both individual and societal points of view.

3.2 The Routine Activities Theory (RAT)

The Routine Activity Theory (RAT) was developed by Cohen and Felson in 1979. They argued that for crime to occur, three elements needed to be present: a Motivated offender, a Capable guardian, and a suitable target. The theory considers crime to be normal and depends on the opportunities that avail themselves for crime to occur. However, crime can only occur if a likely offender thinks a target is suitable and a capable guardian is absent. It is the offender's assessment of a situation as to whether a target is suitably protected and whether the reward is appealing enough for the crime to occur. Moreover, RAT contends that any individual can commit a crime when an opportunity presents itself. For instance, the individual does not need to be a hardened criminal or convicted offender to be a capable offender (Kigerl, 2012 & Olayemi, 2014).

Maimon, Kamerdze, Cukier, and Sobesto, (2013) note that Cohen and Felson initially developed the theory to explain terrestrial crimes. They found that terrestrial crimes, such as violent or property crimes, mostly occur during the early morning or late evenings. The offenders act on rationality; they intentionally target, take, or destroy the property of a victim. They often target property and houses without security or guardianship to decrease the risk of being caught. This shows that the "temporal distribution of routine activities exposes physical environments and their users to varying crime levels" (Maimon et al., 2013:325).

3.2.1 Rationale of RAT to Cybercrimes

Although RAT was initially developed to explain street or terrestrial crime, the researcher has also found the theory equally applicable to virtual crimes. The theory is relevant to this study in the sense that it provides a significant understanding of cybercrimes and its policing. Moreover, it elucidates who engages in crime, who the cybercrime targets are, and who responds to these crimes (Olayemi, 2014). In this study, cyberspace extends the real world, where political, economic, social, and cultural interactions occur. This is not to argue that the physical (or environmental) spaces and cyberspaces are the same and should be treated similarly, but instead that there is no intractable difference between them. However, the role of the RAT in the applicability of cybercrimes is still open for discussion among criminologists. Researchers are at an argument that there is still a need for criminological theories that can explain or support the emerging challenges that occur in cyberspace (Ogunlana, 2019). The three most crucial elements of RAT are then explained to understand cybercrimes: The motivated offender, the suitable target, and the absence of a capable guardian.

3.2.2 The Motivated Offender

Cohen and Felson, 1979, consider a motivated offender as an individual with intent and the ability to commit a crime. Offenders have various reasons to commit crimes. A target must possess something desirable or attractive to the offender (Holt' & Bossler, 2013). Furthermore, for crime to occur and be successful, the offender must be able to commit the crime, and there must be nothing hindering the motivated offender from carrying out the crime. A motivated offender in cyberspace can be anyone connected to the internet to conduct illegal activities. It could be fraudsters, hackers, stalkers, etc. These offenders spend much time online to stay active and ensure maximum exposure to potential victims (Holt' & Bossler, 2013). Technological advancements have allowed criminals to conduct their activities easily and in the comfort of their homes, eliminating the need for travel (Hjertstedt, 2019). Daily computer activities, legal or illegal, place individuals closer to motivated offenders, similar to how daily activities may place individuals in a physical space. Criminals engage in activities such as child pornography, hacking, stalking, or scams for financial gain, revenge (such as cyberbullying or taunting of someone’s image), and fraud (Li, 2018).

Mabaso (2018) states that about five billion people are connected in cyberspace, with almost 50 billion technological devices being adopted, and Criminals are exploiting this connectivity. The growing internet infrastructure is causing law enforcement challenges and making it easier for cybercriminals to carry out their illicit activities.

It enables them to swiftly and inexpensively send a large number of emails (Phishing) to a worldwide pool. Offenders can target victims in nearby places and abroad (Baylon & Antwi-Boasiako, 2017). Moreover, the ease with which cybercrime crosses national borders, the irreconcilable differences between national legal frameworks, and the deceptions employed by cybercriminals impede attribution and prevent law enforcement agencies from interrogating suspects and apprehending offenders (Mugisha 2019). The offender's goals and abilities concerning the target's inherent qualities determine the appropriate target. Experiences and success may also increase the likelihood of a person's tendency to commit a crime (Mabunda 2021). It is also important to note that an individual may commit a crime unintendedly or indirectly in cyberspace. For example, a person who uses or owns a computer may access or find confidential information not belonging to him or her, which may be a breach of privacy. At the same time, others may access personal information for the sole purpose of committing a crime. This supports the theory that anyone can commit a crime when the opportunity arises and does not need to be a hardened or experienced criminal. The Suitable target is the second component needed for a crime to occur.

3.2.3 Suitable Target

The suitability of the target to the offender is usually determined by the vulnerability associated with the target. Cybercrimes may be associated with the time spent on the internet and the types of activities an individual engages in while online (Navarro & Jasinski, 2015). Suitable targets can be individuals, companies, and government agencies that utilize the Internet. Their connectivity increases the risk of being targeted by cybercriminals. High-risk factors include providing personal information, accessing unidentified websites, and engaging in business online. Vulnerability is further increased by internet users' ignorance about cyber security. These risks can be decreased by effective cybercrime policing (Ismail, 2020).

Choi (2008) and Mabunda (2021) mention the below four main criteria that determine the suitability of a target and for the successful execution of a crime.

Namely, the value of the target, inertia, accessibility, and physical visibility of the target (VIVA).

I. **Value**

Social and economic context determines a target's monetary or symbolic value. A target can include digital code and information. An offender can invade a target's computer system to gain information, spreading malware and causing viral damage. Additionally, an individual may be bullied or stalked because they are members of a certain social, racial, ethnic, or religious group. The offender's assessment of the targets determines their value.

II. **Inertia**

The physical characteristics of a target are known as inertia, and they are inversely correlated with suitability. Because of technology advancements, virtual property may appear weightless, but it still has inertial properties. Technological developments have allowed material to be downloaded and copied almost instantly; pirated content, such as music and movies, is clearly illustrative. The amount of data may be a barrier to suitability, particularly when there is a weak internet connection. The motivated criminal also needs the right equipment to complete their illicit activities.

III. **Visibility**

Since an offender needs to be aware of the existence of a target to commit a crime, the RAT theory contends that visibility and suitability for offenses are positively correlated. In cyberspace, visibility is not constrained by physical distance. A visible person or property is more likely to be a target. The public aspect of the internet makes present objects worldwide visible and attracts the most significant number of criminals. Because social media and social networks are so widely used and interconnected, more individuals are at risk of becoming victims of cyberstalking and cyberbullying.

IV. **Accessibility**

Another important consideration when assessing a target's eligibility for a crime is accessibility. The non-linear aspect of cybercrime makes it appealing since it escapes quickly and simply. However, security features like invasion detection systems can still be used to detect cyber

offenders.

Tools like third-party servers and encryption devices can be used to get around this. Indeed, the Suitability of a target applies to crimes in cyberspace. When an individual connects to the internet, confidential information on the computer inadvertently transports valuable information into cyberspace, attracting offenders. Moreover, if the motivated offenders possess sufficiently capable computer systems, the target's inertia in cyberspace becomes almost weightless. And because of the nature of cyberspace, the easy access, availability, and visibility of the internet, motivated offenders can detect, target, or commit cybercrimes from anywhere in the world (Choi, 2008). Therefore, although using the internet can be considered fast and effective, it can also be regarded as unsafe behavior. Maimon et al. (2013) argue that technology-related crime changes the nature of victimization. It effortlessly brings the offender and victim close. In space, victims have a high chance of coming into contact with certain groups and their members that may encompass a share of offenders.

The lifestyle and socio-demographic factors of an individual also play a role in the chance of victimization. Race, age, sex, or even marital status have been some of the important predictors of the possibility of becoming a victim of violent crimes, similar to how some of these factors affect online offending. Maimon et al. (2013) postulate that both legal and illegal online activities may factor in online victimization. An online illegal activity or lifestyle may include downloading pornography or digital piracy. At the same time, a legal online lifestyle may consist of constant online purchasing or cloud meetings. These activities may increase a person's risk of cyber-victimization, such as internet fraud, malware, and online harassment. The target's attractiveness may also be based on the size of the networks, the population size, and users. A suitable target may also be associated with and determined by the type of environment one moves around in, such as a job or even a school. Maimon et al (2013) argue that (as cited in Yar 2005) it may be a bit challenging to think that the convergence in time and space is similar in cybercrime and terrestrial crimes. This is because cyberspace is continuously populated and makes it difficult to easily predict when an individual will be expected to engage or not engage in online activities. This argument could be especially considered nowadays, as the use of the internet, the development, and access to technological devices continue to increase immensely globally. However, it can also be argued that there are instances where computer networks are more active. These may be seen at specific times of the day (in

universities, schools, companies), weekly (commercial entities), or even monthly (small business billing cycles).

These particular computer activities may expose or increase the risks of systems attacks. For example, universities usually experience a higher density of computer use or computer networks during the day. Therefore, they may most likely be exposed to computer attacks during regular business hours. In other words, universities may experience more cyber-attacks during working than non-working hours (Maimon et al. 2013). Spending so much time online is part of their daily routine, which can also expose them to victimization. Moreover, unlike physical crimes, everyone connected to the Internet is a suitable target for most forms of cybercrime. The target's attractiveness may include the time spent online, social network sites, use of online purchasing pages, banking, etc. Many people engage with strangers online and often neglect to update anti-virus systems, and these risky behaviors put them at a greater risk of being victimized (Li, 2018). An individual's actions, patterns, or lifestyle put them at risk. Individuals are also targeted due to a lack of cybersecurity awareness, computer illiteracy, and language barriers (Baylon & Antwi-Boasiako, 2017). The absence of a capable guardian also determines whether a crime will occur.

3.2.4 Absence of Capable Guardian

RAT asserts that victimization is, in part, the result of the absence of a capable guardian. Guardianship from offenders' perspective may vary from visible security guards, parents, school principals, law enforcement officers, landlords, etc. In relation to the study, law enforcement, network administrators, users, and a range of automated protections like firewalls, virtual private networks, anti-virus, and anti-intrusion software are considered guardians (Ismail, 2020). An offense may only be successful without a capable guardian. In Cyberspace, activities have more to do with the effectiveness of indirect guardianship and, therefore, may motivate crime (Olayemi, 2014). Society depends heavily on technology for almost everything in life, and billions of people are now connected to the internet, using their computers and smartphone devices. The absence of a guardian could mean the lack of technical, formal, and informal controls to prevent cybercrime. Users often play a primary role in the prevention of cybercrime. Users who lack knowledge of available measures to reduce the risk of cyberattacks expose themselves to cyberattacks. It is, thus, very important for all users to have some knowledge of computer technology, limit interactions with strangers online, and

update operating and anti-virus systems regularly (Li, 2018).

The advancement and development of technology also create challenges for law enforcement officials in investigating cybercrimes. While law enforcement officials need to keep abreast with cyberspace technology, it is also important for them to adapt their investigative techniques to fit the cyberspace world and protect the public. For example, to investigate and convict sexual offenders, investigators have to develop proactive investigative measures. Such measures may include undercover operations, for instance, targeting child pornographers, individuals who educate minors about sex, and following online criminal complaints (Navarro & Jasinski, 2015). Li (2018) argues that there are instances where guardians can be present but unable to prevent crime. For example, law enforcement officers play a role in reducing cybercrime. However, they are often restricted by conflicting international laws, a lack of equipment, and the proper understanding and knowledge of cybercrime. Mabunda (2021) also points out that police officers are unlikely to be present during crimes and are not always accessible to monitor cyber offenders. As a result, fresh perspectives on law enforcement and cybercrime prevention are required. Because of the scale of the internet, cybercrime requires new strategies for both law enforcement and prevention. The police ought to adjust to the evolving criminal environment.

The absence of guardianship means that a crime is more likely to occur (Miller, 2013). Unclear guidelines and ineffective legislation to prevent cybercrime are also a challenge. Capable guardianships, such as a variety of installable automated protection systems or software, such as anti-virus software, ID authentication, firewalls, and so on, can be adopted by individuals to safeguard computer systems (Li, 2018). However, unauthorized intrusion, malicious software, and interference can compromise and disrupt these systems or structures. Moreover, Holt and Bossler (2008) are of the view that these forms of computer programmes are not meant to deal with compromising or risky communications. It is the responsibility of the individual, department, or company to update protective software and constantly reduce the chances of victimization.

3.2.5 Criticism of the RAT

Although criminologists and/or criminological research have empirically supported the theory,

fundamental criticism still resides among scholars. The routine activities theory is often criticized for how it deals with crime. The theory focuses on three elements to explain crime: the motivated offender, suitable target, and capable guardian, but tends to disregard the social dimensions of criminal behavior. Examples of these dimensions may include personal education and socioeconomic status (Choi, 2008). There is also a notion that the routine activities theory focuses on describing crime and does not explain crime. The routine activities theory is also regarded as an extension of Hindelang et al.'s 1978 lifestyle-exposure hypothesis. In other words, routine activities theory is a theoretical extension of lifestyle-exposure theory. It embraces the core tenet of lifestyle-exposure theory, namely, the individual's professional and leisure activities. Cohen and Felson, 1979, appear to have absorbed this tenet into their acceptable target tenet, adding a motivated perpetrator and a lack of capable guardianship. While some scholars have identified some critics, according to Choi (2008), there is no doubt that the theory effectively explains why particular categories of people are more likely to commit crimes and why certain types of crimes are more common.

In relation to the study at hand, the routine activities theory was initially developed to explain terrestrial crimes. When this theory was explained, there were no cyberspace challenges or the surge of the internet, and the theory mainly disregarded crimes that do not occur in a physical location. There is no physical contact in cyberspace; however, victims, targets, and offenders can meet virtually without physical interaction. This then questions the theory’s relation to victimization in a cyberspace setting. Some scholars argue that although the victim and offender interact through a system or network, the disparity in space between target and offender can be reconceived in this light to explain opportunities. Some scholars have argued that the RAT is unsuitable for the application of cybercrimes (Holt, Turner, Freilich & Chermak, 2021; Choi, 2008; Reyns, Henson & fisher, 2011). They argued that the Spatio-temporal convergence of the theory is questionable to the virtual nature of the internet. For example, an offender is never in physical contact with the target. Moreover, because of the nature and constant demand of the Internet, any public-facing website, server, or system may be visible to an offender as a target and can be accessed anytime. Target's inertia is also undermined in cyberspace, as the speed of one's Internet connection allows large-scale downloading and uploading of content to affect targets of nearly any size (Holt et al, 2021).

Despite the criticisms, the RAT is still considered applicable to cybercrimes. Empirical tests on studies of RAT and cybercrimes have allowed the RAT to be used as the new theoretical application for primarily explaining computer crime victimization (Choi, Scott, and LeClair, 2016, Holt et al 2021 & Williams, Levi, Burnap & Gundur, 2019). The RAT posits that an appealing target and a lack of a capable guardian must interact with a motivated criminal in time and space for crime to occur. This point of understanding is especially useful to cybercrime because it does not rely on complicated understandings of perpetrators' motivations. However, Williams et al. (2019) maintain that researchers have rarely focused on offenders' motivations to commit cybercrimes because of the low levels of law enforcement to apprehend or prosecute offenders. The following criteria were shown to be relevant in predicting victimization in one of the earliest analyses of RAT as applied to cybercrime: Target visibility, as a result of the frequency and variety of online routine activity and target accessibility, increased by the lack of a capable guardian (Williams et al, 2019 & Williams, 2016). Williams (2016:23) also supports and states that "concerning the central core concepts of RAT, motivated offenders, and capable guardianship could be treated as largely similar between cyber and terrestrial settings."

Studies conducted in the United States, United Kingdom, Europe, and the Netherlands on online activities such as online shopping, online banking, emailing, and downloading have been found statistically relevant in predicting online victimization and identity theft. Recent studies that have been done on cybercrimes have been supported and/or facilitated by the RAT, predicting the relevancy of target visibility and accessibility to online crimes (Reyns, 2013). Furthermore, Holt et al. (2021) state that in the case of hacks and malware infections that enable data theft and fraud, cybercrime investigations frequently focus on offenses with a clear instrumental purpose for the offender. Offenders are motivated by monetary gain or access to sensitive data. Some offenders may engage in cybercrime to showcase their expertise or gain social approbation from other members of the hacker community. However, it must be noted that the applicability of a suitable target is still challenging for researchers as the theory postulates that the organization of time and space is central to criminological explanations. Williams (2016) suggests that to deal with this challenge, the RAT can be expanded to account for crimes where the offender and target do not occupy the same physical space. The RAT can be modified to include shared networks (such as the internet) for motivated offenders to reach

targets through this network.

3.3 Structural Functionalism Theory

The functionalist school asserts that social structures fulfil specific demands and that functional imperatives must be met for a community to survive. A function is defined as the fulfilment of a need. Societies, like biological beings, have needs that are analogous to an organism's biological needs. Following this rationale, one wonders what needs are needed for cyber systems and what happens if these needs are not met (Chilcott, 1998).

3.3.1 Background of Structural Functionalism Theory

Pasaribu (2018) points out that the structural functionalism theory is the most influential theoretical building in the social sciences of the twenty-first century. Structural functionalism originates from the writings of Talcott Parsons and Robert K. Merton in the 1930s. One of the essential assumptions of the theory is that society consists of systems. These systems are made up of interdependent parts and cannot function without one another. Any changes from one part will cause an imbalance, resulting in changes in the other parts. “It maintained that society is an organism, a system of parts, all of which function together for the overall effectiveness and efficiency of society” (Olayemi, 2014:119). According to Pasaribu (2018), The theory is mainly guarded by biological thinking, which views society as a biological entity of interdependent organs. The dependence results in the organism’s survival. This functional structural approach, like other practices, strives to produce social order. In other words, society must have balance to survive and function. Society is integrated when members agree on certain social principles, norms, or beliefs that may transcend differences. Cohesive integration will result in the society being perceived as a functionally integrated system and in a state of balance. Any time one of the organs malfunctions, it is thought that this malfunction will impact the organism's life. The theory, therefore, views society as a collection of interconnected and interdependent social structures (Pasaribu, 2018 & Enweonwu, Ugwu, Onyejegbu, Areh & Ajah, 2021).

Robert K. Merton also added to the Structural-Functionalist School of Thought that social patterns, institutions, and structures have latent and manifest functions. Implications or outcomes of the manifest functions are anticipated, intended, planned, expected, envisioned,

and have recognized challenges or outcomes. These are activities that the community expects institutions to do, and they are not surprised when these functions, outputs, or consequences occur. The latent functions look at the "unintended, unplanned, neglected, extemporaneous, spontaneous, and unfamiliar consequences" (Abdul-Rasheed et al., 2016). For instance, the development of technology is intended for social and economic development. However, it has resulted in the latent function being executed to perpetrate cybercrimes. Therefore, sociologists must study, analyze, or examine the apparent and hidden functions of social patterns, structures, and institutions. For example, in online fraud, the manifest function provides cybercriminals income while dysfunction causes financial strain to the victim. Latent functions result in dysfunction and harm to both the victim and the offenders' countries' external image (Abdul-Rasheed et al., 2016).

Pasaribu, (2018) Mentions four conditions that must be met for society to function. These include Adaption, Goal, Attainment, Integration, and Latency, which refers to the four needs (AGIL). The community must accomplish the AGIL functions to survive, namely.

I. **Adaptation** -is a system's ability to cope with changing external circumstances. The system must adapt to its surroundings as well as its requirements.
II. Achieving the system's ultimate **Goal**, i.e., defining and achieving the system's ultimate goal.
III. **Integration**- a system that must control the interrelationships of parts that eventually become components. The system must also manage interrelationships between the other three significant functions.
IV. **Latency**. i.e., equipping, maintaining, establishing, and maintaining motivation.

Parsons views the system structure as both a challenge and a tool for change. Changes in system structure occur in a rather smooth manner. Individuals interacting with common goals can change situations by adopting the role of the "bargaining process." Once their role is established, they can form norms that guide subsequent action and thus become customs that stabilize social interaction (Pasaribu, 2018).

3.3.2 Rationale of the Structural Functionalism to Cybercrimes

Merton's writings assert that crime and deviance are necessary parts of social organization

(Olayemi, 2014 & Abdul-Rasheed et al., 2016). To maintain the effective functioning of a society, the society must cohesively instill organizational structures to control and maintain social order. Society must share the same values and norms to bring about stability. Idowu (2021) affirms that society's social and sociocultural structure are the causes of deviant conduct (cybercrime). In anomic societies, it is characteristic to pursue achievement even with limited resources, which worsens instability and imbalance. Merton asserts that people in later societies tend to disregard the rules and pursue achievement by whatever means necessary. The inability to maintain societal expectations or achieve goals causes an individual to engage in criminal conduct (Olayemi, 2014). Moreover, deprivation of opportunity and people's responses to anomie are influenced by where they are in the social hierarchy.

There is an increased use of technology for socio-economic development, but it is inversely used to perpetrate criminal activities. The apparent function of cybercrime is predominantly fraud, providing income for cyber offenders while causing financial loss to the victims (Abdul-Rasheed et al., 2016). Idowu (2021) states that normlessness arises when regulations stop being followed, which promotes cybercrime. The public experiences cyberbullying, identity theft, and more. All these factors combine to create a disorganized system that negatively impacts the country (Enweonwu, Ugwu, Onyejegbu, Areh & Ajah, 2021). Structural functionalism theory asserts that the family, the education system, the government, the police, and the economy are all interconnected and dependent on one another. These elements carry out a variety of tasks to preserve, uphold, and sustain the social structure. Issues with a particular aspect might impede the development of other parts. Crime, unemployment, poverty, and social influence are unavoidable parts of the system that collectively affect how effective and efficient society is (Alabi, Bamidele & Oladimeji, 2023).

Alabi, Bamidele, and Oladimeji (2023) argue that the cause for the increase in cybercrimes is structural failure and the inefficiency of the legal system. South Africa has responded to the challenges associated with cybercrime. For instance, it has introduced several security laws or legislation, such as the Cybercrime and Cybercrime Bill and the Protection of Personal Information Act (POPIA), to prevent cybercrimes (Capazorio and Hollis, 2017 & Lourie, 2015). These laws were developed in an attempt to preserve social balance by ensuring institutions fulfil their daily obligations and duties to lessen societal misconduct. However, these strategies have been criticized for being unclear and progressing slowly. Another

challenge, according to Rustad (2001), is that bringing about stability in cyberspace is a challenge for law enforcement officers.

The police officers struggle to keep up with the pace of the growth and advancement of technological systems. Therefore, they cannot effectively deal with the sophisticated cybercriminal subcultures in the anonymous offshore spaces. Cybercriminals can equip and advance themselves with new software tools to attack computer systems immediately after they learn of the changes or updates on internet-related criminal laws. Alabi, Bamidele, and Oladimeji (2023) argue that the theory tends to disregard the disadvantages that certain people experience due to uncontrollable circumstances. Because not every member of society has access to opportunities, this results in injustice and bias. The imbalance in opportunities causes cybercrimes. Moreover, the goal of combating cyber-criminal offenses in South Africa is hindered by the failure of developmental structures and institutions of governance (such as limited law enforcement agencies) to function efficiently. Law enforcement officials still deal with cybercrimes uncoordinated and fragmentedly and rely on other common law cases (Kempen, 2019).

The country still lacks the knowledge and expertise in the cyber field. Therefore, strong social organizations, governance, or legal systems must be developed, and the existing structures strengthened to achieve efficiency and prosperity in decreasing cybercrimes. Increased use of private investigators and other stakeholders in law is paramount in reducing the enforcement gap in apprehending and prosecuting cybercriminals. The government should enact strong laws and create institutional frameworks to enforce law and order (Matthew, 2016 & Lourie, 2015). Cybercrime legislation, sentencing, and probation guidelines must be reviewed to address the rapidly evolving cybercrimes. Sentencing guidelines must be clear and direct when prosecuting offenders (Rustad, 2001). Moreover, cyber offenders from African countries often engage in cybercrime mainly for financial gain. This could suggest that there may be a need to strengthen the existing governance structures, provide job opportunities, and decrease poverty levels to reduce the number of cyber-attacks (Bestoyin, 2018). Although the functionalist schools bring sound arguments to the study, some criticisms or shortcomings come with the theory.

3.3.3 Criticisms of the Structural-functionalism Theory

The structural-functionalist theory comprises two significant criticisms. It has been criticized

for presenting a static or entropic picture of society, and it portrays the incapacity to account for or deal with social change. It also overemphasizes integration and fails to deal with dysfunction (Chilcott, 1998).

According to Morrow (1978), conflicts or opposition predict that a given structure will change. A better understanding of the dialectical process and how maintenance mechanisms work to defeat dialectical mechanisms and modify them will determine a change. Demerath (1966) also mentions three sides to the structural-functionalism argument. The ones who stand by the school as a distinct approach to sociological phenomena. Secondly, those who critic structural functionalism with conflict assumptions. Those who believe that all science is structural-functional, that disputes must be avoided, and that more focus should be on the analysis. Although there are evident contrasts between these perspectives, there is also some common ground. Each of them tends to see structural functionalism as a unified entity. Each considers it to be a single theoretical position that can be assessed in its entirety (Demerath, 1966). To overcome the critics, Chilcott (1998) proposes that functionalists view function as a verb rather than a noun by focusing on the process of institutionalism rather than the institution itself. Furthermore, the theory contends that certain norms and principles guard society but cannot explain how customs came to be. Despite these objections, the functionalist theory provides problem-solving approaches that can provide feedback to the police as to what is missing and needed to deal with cybercrimes effectively.

3.4. CONCLUSION

The police force is one of the most crucial fighting institutions. When the police fail or are ineffective in their part to reduce and/or control crime, the whole system breaks down. Therefore, these further damages the trust between the public and the police force. Cybercrimes have been one of the growing challenges for law enforcement personnel. The RAT and structural-functionalist theories then assist us in understanding the deriving factors of cybercrimes and how these can be reduced. The RAT argues that our routines can put an individual at risk of victimization. The three elements (motivated offender, suitable target, and lack of capable guardian) must be present for a crime. The Theory also allows the researcher to discover and understand the varying types of crimes (such as online fraud, phishing, illegal pornography, etc.) encompassing cyberspace. The central arguments also come from the Structural functionalism theory. The functionalist theory is very suitable for analyzing

cybercrimes in South Africa. The central argument of Structural Functionalism is that the degree to which a given political system can perform its functions effectively will determine not only the level of its stability but also its prosperity.

A country whose institutions can perform their roles effectively will achieve political or governmental stability and development. A country whose institutions are weak and, as a result, cannot perform these roles efficiently will experience conflicts and instability.

CHAPTER FOUR

RESEARCH METHODOLOGY

4.1 Introduction

This chapter describes the methods used to address the research problem and/or the study's research questions. The researcher aims to reveal the law enforcement officers' experiences in responding to and knowledge related to cybercrimes in South Africa. Goundar (2012) states that it is imperative that the researcher possesses knowledge of both methodology and research methods or techniques. Additionally, the researcher must understand which of these approaches or strategies are relevant, which are not, and what they signify and suggest. To illustrate how data was obtained, a qualitative research approach was considered appropriate for this study. A purposive sampling method was employed, and data collection was in the form of in-depth interviews. Data was analysed using the thematic analysis process. The study's ethical considerations and limitations encountered by the researcher are also outlined in this chapter.

4.2 Research Paradigm

Qualitative research is founded on the interpretivism and/or constructivism paradigm. It posits that there is no access to reality outside of our thinking; reality is socially constructed and ever-evolving. Gishuru (2017) states that a research paradigm consists of three components that interpret a particular worldview: epistemology, ontology, and methodology. Epistemological assumptions relate to presumptions about how we learn about the world; ontological beliefs are our ideas about reality or the nature of reality (Gishuru, 2017). The methods include what is chosen to accomplish our goals and the methodological choices. The paradigm of this study assumes a subjectivist epistemology, a relativist ontology, and a naturalist methodology.

The interpretative paradigm of the study seeks meaning and examines the complexity of the human world's subjective experience and social reality. It aims to define people's environments, interactions, and experiences. In the investigation framework, the researcher and the subject of the study are dynamically linked, generating shared findings within the context of the investigation (Goundar, 2012). The study utilized focused samples to obtain insight into people’s reality and thoughts. Naturalistic inquiry and qualitative research techniques, such as in-depth interviews, were the foundation of this methodology. In-depth interviews allow for honest, complex responses, and skilled researchers employ various strategies to get detailed information.

In this study, data was collected through semi-structured interviews; the data was then systematically analysed to interpret meanings. This process yielded rich, detailed data with insights impossible with quantitative research methods (Goundar, 2012). Gishuru (2017) states that bias in individual researchers may be reduced by using techniques like triangulation. Researchers who employ interpretivism recognize that their issues are social in nature and that society is a human construct with qualities that are neither observable nor quantifiable (Gishuru, 2017). In this research study, the constructivism paradigm was employed to understand the constructed realities shared by the participants on the topic under study.

4.3 Research Approach

A qualitative research approach was adopted for this study. The qualitative research approach was the most appropriate and convenient approach for answering the previously mentioned research questions as it sought subjective opinions or views of the participants. Kalu & Bwalya (2017) state that understanding people's cultures, ideas, values, and experiences is the main goal of qualitative research and aims to create theories that explain these experiences. Goundar (2012) defines qualitative research as a quality-related qualitative phenomenon that studies the socially constructed aspect of reality. It studies the close interaction between the researcher, the participant of the study, and the situational restrictions that shape the investigation.

The researcher wanted to gain a deeper understanding of cybercrimes, police experiences in dealing with and how they respond to cybercrimes. The qualitative approach comes from the behavioral and social sciences. It aims to understand the underlying reasons for actions and how they eventually influence people's lives by using the words of participants and researchers to explain the phenomena being examined (Astalin, 2013; Goundar, 2012 & Hassan & Khairuldin, 2020). Qualitative data allowed the researcher to better understand the phenomenon under study, producing imperative and substantial results. It was chosen because it does not generalize or reduce the findings into statistical and quantifiable concepts. This approach is also considered suitable for studies on cyber-related crimes. It helped create a space where participants could contribute knowledge based on their unique experiences. Qualitative research gave a more profound and in-depth understanding of the police perspectives and their experiences with cybercrimes (Nkosi, 2018).

Furthermore, this method allowed the researcher to be immersed fully while being very attentive to new insights in the process of gathering data. In qualitative research, the data are seen or heard directly from the source, and readers can readily relate to the findings. Hence, the researcher chose this flexible, highly focused, and efficient technique. Moreover, because of the descriptive, narrative nature of qualitative research, the study allowed the researcher to look at different kinds of knowledge that would not have been available, which led to new insights (Goundar, 2012).

4.4 Research Design

A research design is a systematic plan of action that involves all steps necessary to accomplish the study's goal and acts as a planning framework for research. It is a detailed plan for gathering and analyzing data, which are two more aspects of social science research. A research design ensures that the study is concluded and reaches its goals (Hassan & Khairuldin, 2020). This study adopted a Phenomenological research design. Phenomenology design aims to explain the meaning, structure, and essence of lived experiences around a specific phenomenon. It aims to understand people's viewpoints, perceptions, and knowledge of the issue (Vinay Chandra Pathak, 2017). This design was appropriate for this study as it seeks to understand police officers' understanding, perceptions of cybercrimes, and experiences in responding to them.

According to Errasti-Ibarrondo, Jordan, Dıez-Del-Corral, and Arantzamendi (2018), Phenomenology works best when the study question necessitates an in-depth understanding of a common human experience. The focus is on individual perception and knowledge of the topic under study. Phenomenology is also employed to research fields in which little is known. To comprehend the lived experience from the subject's point of view, researchers must set aside their own opinions and sentiments. This procedure makes it possible to understand the phenomena better. Indeed, the phenomenological study allowed the participants to express themselves fully through in-depth interviews and in their own words to understand their subjective experiences of cybercrimes. The police officers involved in the study had firsthand experience and knowledge of cybercrimes and investigating online crimes. The participants could give a detailed description of the phenomenon under study. Furthermore, by providing phenomenological research an interpretative component, it becomes possible to utilize it as the foundation for helpful theory, which in turn influences, supports, or may contradict action and

policy (Errasti-Ibarrondo et al., 2018). The participant's views were interpreted to describe the police officers' experiences and how they are constructed or create meaning. This design allowed the researcher to gain detailed information and better understand the nature of the issue being studied. The police officers were able to adequately articulate how they address cybercrimes caused by the constant changes in technologies.

4.5 Location of the study

The study was conducted in Durban (CBD), KwaZulu Natal, South Africa. KwaZulu Natal is one of the nine provinces in South Africa with an estimated population of 12.34 million, which is the second biggest population in South Africa (Stats SA, 2024). Durban is located on the Eastern coast of South Africa and is a diverse city. According to Masthead (2020), South Africa ranks third globally in cybercrime victims, with an estimated annual loss of R2.2 billion due to cyberattacks. Internet connectivity is a significant contributor to the risk associated with cybercrimes (Masthead, 2020). South Africa is now much more digitized than it was 20 years ago. There are over 31.18 million internet users in South Africa. Most of the internet users reside in cities and large towns (Harrison, 2019). KwaZulu Natal (KZN) has the second largest number of internet users (at 16,68%) in South Africa. While the city of Durban has the third largest (at 10,65%) of internet users (Harrison, 2019).

Barret (2013) Explains that the challenge with the increase in internet use is that many people are unaware of the actual presence of cybercrime and the huge risks it poses to them. The South African public does not know how they expose themselves and how to protect themselves from cybercrimes (Barret, 2013). It is evident that Durban is one of the biggest cities and has a high increase in internet connectivity; therefore, there is a high risk of cybercrimes. The location of the department or police stations that deal with cybercrimes further precipitated the location of the study. The SAPS divisions or units that deal with cybercrime cases in KZN are in the central part of Durban. There are limited government offices that specifically deal with cybercrimes in South Africa. Therefore, the researcher is mainly directed by the location of the specific police units.

4.6 Population and Sample of the Study

A population is a collection of people, objects, or events that are the subject of a study (Garg,

2016). Researchers need to determine if every reference or target population member chosen may be investigated (Garg, 2016). The population of this study involved police officers from the South African Police Service (SAPS) in KwaZulu Natal, Durban. Qualitative studies use a smaller sample to explore a phenomenon in-depth and discover more reliable data. The sample selected represents a specific population where certain characteristics may be studied to understand the entire population (Nkosi, 2018).

SAPS has different divisions, and police officers who encounter cybercrimes usually direct those crimes to units and officers who specialize in that field. Therefore, care was taken to ensure that the chosen participants accurately reflected the whole population to acquire and discover relevant information (Nkosi, 2018). One of the biggest challenges that South Africa and law enforcement agencies face is the shortage of "security manpower" and the lack of skills in technology-related crimes and forensic investigations. Therefore, there are about a few law enforcement officers who deal with cybercrimes (Nkosi, 2018). The number of participants is, therefore, lower. The research aimed to select twenty-five (n=25) law enforcement officers for this study. However, only seventeen (n=17) officers could be accessed for the study. This was a lower number of participants than anticipated. This was because not many police officers had knowledge of the topic under study or experience. Some experienced police officials were about to retire, which indicated that there would be even fewer police officials who deal with cybercrimes and have experience. The participants were accessed through the Durban Commercial Crimes Unit and Directorate for Priority Crime Investigation (DPCI). The Commercial Crimes unit was chosen because it is a division that mostly deals with cybercrime cases in Durban, KwaZulu Natal, and works closely with the DPCI.

4.7 Sample Size and Selection

Mason (2010) states that the least appropriate sample size for qualitative research is fifteen. Though these figures are provided as a guide, they often do not include empirical justifications for why these figures and not others are appropriate. Morse's (of 1994), works highlight the importance of considering various critical factors when deciding on the sample size, including the study range, subject nature, study design, investigator experience, budget, and time. This study was guided by the nature or subject of study, scope, and time (Bekele & Ago, 2022). In this study, the researcher conducted 17 (n=17) face-to-face interviews with participants based on voluntary participation.

No participant felt pressured to partake in the study. The study's sample size, chosen from the entire population, plays a crucial role. The participants were from two units (DPCI & commercial crimes unit) in the South African police service that mostly encounter and investigate cybercrimes. Three (n=3) police officials were from DPCI, and fourteen (n14) police officials were from the commercial crime unit.

The participants interviewed had ranks of lieutenant colonels, captains, and detectives. The researcher wanted to interview participants with a deeper knowledge of cybercrimes; this was then easier as many of these officers have been working in the units for years (10 and above years), and some are even about to retire. Only three police officials had recently joined the departments; however, they have been police officers for many years.

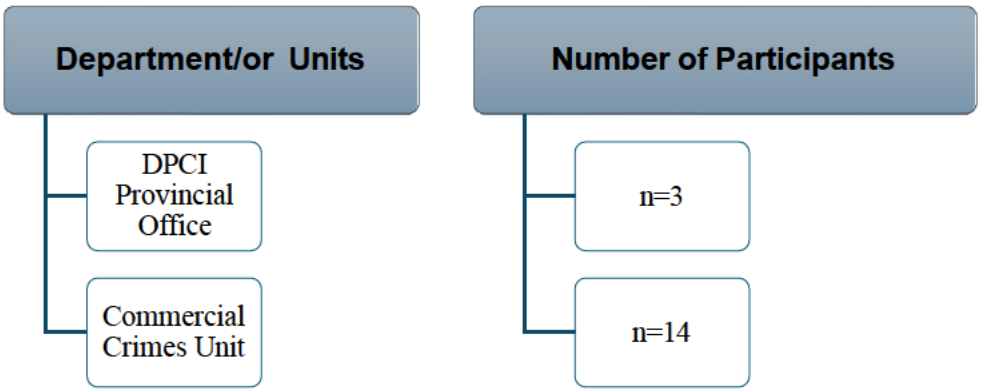


Figure 4.1: Sample Size

4.8 Sampling Frame and Technique

The study adopted the non-probability sampling strategy. This type of sampling is used for explorative and qualitative analyses. Not every individual of the population has an equal and non-zero probability of being chosen for the sample using this approach. The technique that was utilized in this study is purposive sampling. Purposive sampling selects the sample based on the investigator's judgment (Garg, 2016).

4.8.1 Purposive Sampling Strategy

Purposive sampling employs a nonprobability strategy that entails the selection of participants who are a relevant population for the study. Bekele and Ago (2022) define purposive sampling as the deliberate selection of research subjects according to their relevance to the study

questions and how well they address the research questions. These questions direct the process of choosing participants and groups of individuals to be the subjects of the study and subsequently sampled. Purposive sampling is used because it assumes that some people could have differing opinions on the concepts and problems under consideration and should thus be included in the sample (Campbell, Greenwood, Prior, Shearer, Walkem, Young, Bywaters & Walker, 2020). This sampling technique offers advantages such as studying only the population of interest, making the sample homogeneous, or excluding participants at risk of experiencing serious side effects or may not yield the desired results (Andrade, 2021).

This study selected knowledgeable participants who have specifically or directly encountered cybercrime cases. Many police deal with crime, but not all have the skills in digital expertise. Only those officers who had the expertise and resources to respond to online crimes were sampled. Officers interviewed had ten or more years of experience working in these divisions. The selection criteria included availability, desire to engage, and ability to communicate effectively. The goal was to identify participants who possessed specific qualities that would enable them to contribute more effectively to the study, ensuring the most precise and thorough information (Etikan, Musa & Alkassim, 2016). Moreover, since technology is ever evolving, it was interesting to determine if law enforcement officials were knowledgeable and capable of dealing with cybercrime cases. It was also essential to determine if they were adapting effectively to the constant changes in technology and the changes in online criminal behaviours. Criminals are aware that technology constantly changes. Cybercriminals can also adapt or change techniques to commit more crimes without being detected (Brown, 2015). Including police officers who have more experience working with this kind of crime allowed the researcher to understand and find out how such crimes were being handled.

4.9 Sample Inclusion and Exclusion Criteria

Exclusion criteria indicate characteristics that render the population ineligible for the study, potentially affecting the result parameter, whereas inclusion criteria provide consistency and objectivity (Garg, 2016). The inclusion and exclusion criteria determine who can be included in or excluded from the research sample.

The sample that was included in the study:

I. Law enforcement officers with expertise in the field of cybercrimes
II. Five or more years of experience and knowledge in law enforcement, responding to and investigating online crimes. The majority of the participants in this study had 10 years and more experience. Only a few had 5 years or more experience.
III. Be an officer in the units/ department in KwaZulu Natal, Durban, that deals with online crimes.
IV. Be willing to participate in the study

4.10 Recruitment Plan

The researcher used a more direct approach in recruiting participants. After acquiring the ethics letter from the University of KwaZulu Natal and the gatekeepers' letter from the SAPS head office in Pretoria, the researcher was able to utilize the in-contact or person-to-person approach to access the participants (Negrin, Slaughter, Dahlke & Olso, 2022). This was deemed necessary to complete recruitment on time, given that the researcher had a timeline for finishing the research. In the study, the researcher first had a conversation with the receptionist, who advised and directed the researcher to the station commander. The researcher spoke with the commander and explained the visit's purpose, the study's reasons, and the kind of support needed. The commander wanted time to confirm the permission letter and arranged for the researcher to attend the department staff meeting. This was for the researcher to be introduced to the staff and for the officers to be aware and expect the researcher to visit their offices. This allowed the researcher to pre-consent participation, such as the police agreeing to set up meetings and taking their numbers and emails to set up appointments. Although the researcher also used emails to contact the police officers, they were ineffective. Therefore, cell phone calls were a better option. Constant site visits were also utilized.

4.11 Data Collection Methods

The researcher employed secondary and primary data collection methods to meet the study's objectives. There are conceptual and methodological differences between primary and secondary research. Primary research involves collecting original data more thoroughly and methodically. It often consists of the use of questionnaires, telephone or in-person interviews, and direct observation.

Secondary research, sometimes called desk research, synthesizes or summarizes existing studies, often based on study participants or experiments.

4.12 Primary Data Collection

The primary data of this study was gathered through in-depth (semi-structured) interviews.

4.12.1 Semi-structured In-depth Interviews

Semi-structured interviews were utilized in this study. The semi-structured interview was perceived appropriate for this research because it takes flexibility into consideration and allows participants to speak freely, hence giving the researcher a chance to obtain all the information that is relevant to the research questions. Semi-structured interviews allowed the researcher to explore an individual's life narrative. The Semi-structured interviews are flexible and allow for new questions based on interviewees' responses. The interviews had a good balance between main questions, follow-ups, and probes (Ruslin, Mashuri, Rasak, Alhabsyi, & Syam, 2022). The interviews were conducted individually, with each participant. The data that was obtained were police officers' experiences regarding cybercrime.

The researcher utilized a recording device to record all the responses. The researcher first asked for consent from the participants to use a tape recorder to get a complete understanding of their responses during the interview. They were informed that their anonymity and privacy would be respected, and that no personal information would be revealed in the study. All 17 interviewed participants agreed to be recorded. The researcher was able to interview three female officers and 14 male officers, which showed a gender gap in the sample. However, gender disparities were not a factor in this study, and the gender gap had no impact on the study's outcome. Police officers were interviewed in their private offices in the units (SAPS KZN provincial Office, DPCI, and Commercial crimes units), and appointments had to be made as they were not always present in their offices. The participants also made referrals to their colleagues who knew the subject matter and assisted the researcher in making an appointment with them. An interview schedule guided the researcher. The interview schedule used tailored questions and a more directive style, probing questions when needing more clarification or information from the participants. The interviews took approximately 25 minutes to 40 minutes per participant. The participant's personalities, not their hesitation to respond, were the reason for the variation in interview length.

While some participants answered the questions concisely, others preferred to go into great depth and accentuate their points with examples. The interviews were conducted in both English and isiZulu, with mainly English being utilized. The participants were mixed in race (White, Indian and African). Since the researcher is fluent in both English and isiZulu, participants were asked to feel free to use any language they preferred during the interview to reduce barriers in their responses. Participants were not compelled to respond in English. Interviews conducted in IsiZulu were later translated into English as the sole language for this research paper.

4.13 Secondary Data Collection

The study initially portrays the secondary data, which involved collecting, summarizing, or synthesizing existing research (Goundar, 2012). The secondary resources were accessed or collected from journals, relevant e-books, and peer-reviewed articles from the Internet and Online libraries, particularly from the University of KwaZulu Natal Online library. Other sources using search engines included but were not limited to EBSCHO host, Google Scholar, UKZN research space, Sabinet, and Science Direct. The applicability and reliability of all the sources used in the study were considered in this study and its review. The type of data or documents that were accessed was guarded and incongruent with the objectives or research questions of this study. The study used the process of inclusion and exclusion to narrow down the research topic information. This was done by using keywords such as cybercrimes, cybercrimes in South Africa, challenges of cybercrime, types of cybercrime, and systems to combat cybercrime to access relevant information from online sites and libraries.

4.14 Data Analysis

This research study employed thematic analysis to analyse the data. This approach entails examining qualitative data from focus groups or interviews to discover recurrent themes and arrange the data into hypotheses or research questions (Hassan, 2024). Smith and Firth (2011:3) defined it “as an interpretive process, whereby data is systematically searched to identify patterns within the data to provide an informative description of the phenomenon.” The thematic analysis finds and analyses patterns in a data set, often resulting in new thoughts. It requires researchers to stay true to inductive inquiry and prevent the need to shape their assumptions. This analytical approach was deemed appropriate because it allows for describing and interpreting the participant's views.

The thematic analysis emphasizes making the procedure of information study straightforward and outlining the linkage between the phases of the investigation. It allows for a summary of key elements of extensive informational data, pushing the researcher to adopt a very organized strategy for dealing with the data (Nowell, Norris, White, & Moules, 2017). Furthermore, thematic analysis was chosen because it is more accessible and easier to understand or learn. This study emphasizes the advantages of employing various approaches at each stage and offers researchers a six-step theme analysis strategy. With the use of these procedures, the research process becomes more thorough, and the research findings are more in-depth, which makes systematic theme analysis an effective method for analysing qualitative data (Naeem, Ozuem, Howell & Ranfagni, 2023). These steps include creating a transcript and familiarizing it with data, identifying keywords, choosing codes, developing themes, conceptualizing by interpreting keywords, codes, and themes, and creating a conceptual model.

4.14.1 Transcription and Familiarizing with Data

The first step in the research process of theme analysis is to transcribe the material and get familiar with it (Sovacool, Iskandarova & Hall, 2023). Naeem, Ozuem, Howell & Ranfagni (2023) state that researchers must document interviews using word-for-word transcription and high-quality audio recordings or manually identify important points by highlighting trends. Only the most important and relevant data is included in a selective transcript, making it more concise and easier to analyse. The objectives of the study serve as the basis for the analysis, directing the extraction of important information from transcripts instead of dictating certain conclusions. (Naeem, Ozuem, Howell & Ranfagni, 2023). To provide a focused and controlled analysis, effective transcribing entails choosing sections that are relevant to the assessment of the objectives. By ensuring that the data is clear and simple to interpret, this procedure ensures an in-depth understanding of the research. The researcher was able to immerse fully in the data; all audio recordings were collected, listened to several times, and noted down, and transcripts were carefully read by the researcher to become familiar with the data.

4.14.2 Identifying Keywords

Interviews were analyzed in the study to determine the keywords, repeated phrases, and patterns that best capture participants' perceptions and experiences. Finding and presenting the data's most recurring patterns is the goal of thematic analysis. Selected statements or quotes

from the data are categorized with a code. This method implies that keywords are significant or have a purpose in research (Naeem, Ozuem, Howell & Ranfagni, 2023).

4.14.3 Coding

A critical stage in data analysis is coding, in which brief words or phrases are ascribed to data segments in order to convey the main idea, meaning, or subject of the data. This method assists in identifying components associated with research issues and simplifies complicated textual material by converting it into a theoretical form. In coding, keywords are essential because they organize the analysis and help break down large amounts of unprocessed data into more manageable portions. Coding is crucial because text data are dense and require time to interpret. Real data is divided into smaller, easier-to-manage sections, facilitating categorization, theme, and pattern analysis. This procedure aids in identifying pertinent components and developing a thorough comprehension of the underlying ideas by researchers (Naeem, Ozuem, Howell & Ranfagni, 2023). The researcher was able to identify crucial components and themes that were appropriate and able to respond to the research problem, questions, and objectives of the study. the researcher had to Find themes, identify subthemes and sub-patterns, pay attention to recurrent themes in the text, and start to group the findings into several codes. Participants' data were examined for inconsistencies and similarities, and the relevance of these findings in achieving the study's goals was assessed (Sovacool, Iskandarova & Hall, 2023).

4.14.4 Theme Development

The process of developing a theme involves arranging codes effectively in order to identify trends and connections that shed light on the research problem. By developing themes, this stage moves from thoroughly examining codes and categories to a more abstract interpretation. The recurring or frequent presence of these themes does not imply that they are essential to communicated meaning; rather, they represent systematic meanings that connect the study questions and data. The goal of the research is to identify crucial recurring or significant themes in parts of coded text. Created at the first step of data coding, categories are more precise and distinct. Themes, conversely, are more intellectual and abstract and require interpretation (Naeem, Ozuem, Howell & Ranfagni, 2023). A theme derived from a researcher's observations and theoretical knowledge is an essential connection between study questions and data.

By assigning pertinent codes to extracts, themes are applied to data to identify possible patterns. The procedure required the researcher to carefully group relevant codes to extract significant patterns, which calls for analytical judgment and a deep understanding of the data (Naeem, Ozuem, Howell & Ranfagni, 2023). The study theme development is greatly influenced by the approach selected, and a single extract may be given more than one code. The researcher went deeper in their interpretation of themes to find abstract patterns, trends, or connections. combined subthemes into themes and improved the theories or units of analysis and the patterns to which they belong. Irrelevant themes were removed, and the more relevant ones were matched with the findings from the reviewed literature (Sovacool, Iskandarova & Hall, 2023). This process produced a cohesive narrative that links quotes, keywords, and themes and enabled the researcher to comprehend the data and address research issues fully.

4.14.5 Conceptualization

A critical phase in research is conceptualization, which entails establishing and understanding newly emerging social patterns. Using tools like diagrams or models to comprehend their linkages, researchers refine these patterns into definitions that support their findings. The degree of clarity, precision, dependability, application, and theoretical and practical contributions made by these definitions are used to evaluate their quality. Concepts are mental pictures, thoughts, feelings, or other representations of social events. Maps, graphs, and models are examples of visual aids that researchers employ to comprehend their findings. Ideas are defined first, and then pertinent material is interpreted to establish connections between various concepts. Determining the kinds of evidence to support an interpretation and establishing the range of potential meanings are two aspects of interpretation (Naeem, Ozuem, Howell & Ranfagni, 2023). The researcher may expect a set of topics or themes, but more themes surface during data analysis. To make sure the themes were consistent and matched the coded data, the researcher examined them using the procedures outlined in stage four. The topics were identified by the researcher, who also provided accurate working definitions that encapsulated each theme's key ideas.

4.14.6 Creation of Conceptual Model

The creation of a conceptual model is the last phase in the theme analysis process. This procedure, which is frequently directed by accepted ideas, entails producing a distinctive

representation of the data. The model highlights the study's contribution to knowledge and provides answers to the research questions. This stage represents the end of the study; it summarizes all of the conclusions and revelations that were drawn from the data (Naeem, Ozuem, Howell, & Ranfagni, 2023). the researcher had to check and verify all interpretations. The researcher had to ensure the study objectives were met, making this one of the most important phases of the data analysis process. The researcher gave a comprehensive and accurate account of the experiences of the participants in relation to the study questions.

4.15 Ensuring Trustworthiness

Researchers using qualitative methods often must demonstrate that their study is reliable and trustworthy. It convinces both the researcher and readers that the study is worthy of consideration and recognition. Kalu & Bwalya (2017) state that because the two research methodologies (Qualitative and quantitative) treat validity and reliability differently, some readers and quantitative researchers frequently doubt the credibility of qualitative research This study offers a detailed investigation of the key elements of qualitative research, which, when used correctly and objectively, may better support readers assess qualitative work as being accurate (Kalu & Bwalya, 2017). The researcher addressed trustworthiness in the following ways (Anney, 2014):

4.15.1 Credibility

Credibility addresses whether the information collected from participants is credible and whether the data interpreted is of the original and correct views of the participants. Consistency between participant perspectives and the researcher's representation in the study is dependent on the credibility of the research. Researchers need to maintain objectivity and refrain from expressing opinions in focus groups or interviews to minimize facilitator bias. For data accuracy, tape recording and transcription of discussions and interviews are crucial. To guarantee accuracy, transcripts and audio recordings should be compared. Credibility may be further increased by providing a detailed and methodical explanation of the study process, including design, data collecting, and management (Kalu & Bwalya, 2017). The researcher engaged, immersing herself fully, to get an understanding of the participant’s world. Credibility was also maintained through peer debriefing (by seeking support from academic staff, supervisor, and suggestions on the inquiry of the support of the study). The researcher ensured

not to instill ideas or her opinions in the participants but was objective and listened to the participants while learning about their work. when the research or the study is finished, the researcher will send a copy of the transcript to the police officers for review and verification. Check whether their views and/or experiences are correctly articulated and not compromised.

4.15.2 Transferability

Transferability is the degree to which findings are applicable outside of the research setting. Good research ought to yield concepts and outcomes with broad applicability. In qualitative research, generalization is concerned with the richness and depth of data to ensure the conclusions are applicable and meaningful to other situations or people. This may be done in several ways to get a deeper comprehension of the phenomena that are being studied (Kalu & Bwalya, 2017). Researchers can verify the validity of findings by comparing them to the theoretical framework surrounding the phenomena and the research objectives through analytical generalization. A competent qualitative researcher shows how the facts and conclusions are related, elucidating the process by which a strong cross-reference was made and confirming the accuracy of the findings (Kalu & Bwalya, 2017). Accuracy was maintained in this study through detailed and rich descriptions of the study. All information was depicted in the true manner of the participant's experiences and not on the researcher's assumptions and ideas. recording of the participant's responses allowed the researcher to transcribe the original content of responses to analyze data and illustrate the conclusion or results of the research study. This was also to be used for future references.

4.15.3 Dependability

"Refers to the study of findings over time" (Anney, 2014:278). In research, dependability pertains to the consistency of results and the investigator's capacity to adjust to changing conditions in the investigation, plan, or approach. In a social environment that is always changing, it is hard to anticipate or assure dependability, the researcher must provide the reader enough information. Qualitative content analysis, for instance, might make it easier to draw reliable conclusions, offering new insights and useful recommendations for action (Kalu & Bwalya, 2017). To ensure dependability, Participants will be allowed to provide feedback on the study's interpretation and recommendation and to check whether it supports the data received from them.

4.15.4 Confirmability

Confirmability is when the researcher must demonstrate how interpretations and findings of the study were reached. Confirmability refers to the procedures the researcher takes to show that conclusions are drawn from the facts, ensuring dependability, trustworthiness, and transferability. A thorough description of the research methods should be included to enable readers to assess the suitability of the data analysis techniques, ensuring confirmability. A description of the study concept and implementation is required, along with proof of decision trails at every level of the research process (Kalu & Bwalya, 2017). To ensure confirmability, the researcher explained methods, theories, and analytical steps throughout the study. For example, the researcher explained why purposive sampling was used instead of any other sampling method. The researcher maintained neutrality throughout the study. This was done by setting aside potential prejudices and biases (bracketing). Lastly, all information from the start of the research study (such as recordings and documents) to the end will be kept as evidence or referral to show how the researcher came to conclusions.

4.15.5 Reflexivity

It looks at a researcher's self-awareness of data, encouraging the researcher to be conscious of bias and control. It entails educating researchers on how participants impact the researcher and how the researcher is affected by participants and the study process. Researchers might give their work more credibility by considering the study method and comprehending how individual values affect the results (Kalu & Bwalya, 2017). It was important for the researcher to assess their biases and maintain objectivity.

4.16 Ethical Considerations

Research involves collecting information from people and about people. Therefore, the researcher must consider ethical issues that may be encountered in the process. Phenomenological research requires direct opinions or answers that may solicit sensitive information from the participants (Maldonado, 2008). These views and positions are visible since they can be shared with others and organizations. The researcher needs to ensure that participants' integrity is protected. The researcher must guide against any misconduct and indecency that might affect their organization. The researcher must respect the participant's values, needs, and rights (Maldonado, 2008).

Reviewers and authorized organizations evaluate research projects closely to determine their reliability and credibility. Consequently, ethical guidelines must be followed for research to pass the integrity test. Research projects can gain credibility and integrity by adhering to standards that offer privacy, protection, and trust. Participants in a study may face risks. Thus, researchers must ensure that their participants are protected. This involves being guided by ethical principles such as obtaining ethical clearance, ensuring confidentiality, protection from harm, informed consent, and voluntary participation.

4.16.1 Ethical Clearance and Gate Keepers Endorsement

Before any research can be conducted, it is imperative that the researcher receives ethical clearance. The researcher had sent an application to the Ethics Committee at the University of KwaZulu Natal (UKZN) to get permission to conduct the study. Ethical norms and standards are supported by the documents of the Singapore Statement on Research Integrity, 2010, UKZN's Code of Conduct for Research, the Constitution of the Republic of South Africa Act 108 of 1996, and the Occupational Health and Safety Act No. 85 of 1993. The policy states that all University of KwaZulu-Natal employees, as well as graduate and undergraduate students, who do research on or off campus are subject to the UKZN Research Ethics Policy. Additionally, the same ethical framework applies to anybody who is not associated with UKZN but wants to do research with staff and/or students in UKZN. It is the duty of every member of the university community to uphold this policy in regard to the scholarly work they are involved in and to refrain from any actions that may be construed as being in violation of the policy. Ethical clearance for this study was reviewed and granted by the Humanities and Social Sciences Research Ethics Committee (HSSREC/00003010/2021). Any amendments or adjustments to the study require the committee's acknowledgment, endorsement, or approval.

The researcher was also required to request permission and apply for gatekeepers' letters to the South African Police Services (SAPS) research office. The researcher wrote a detailed letter explaining the study topic and its aims. The letter was approved in terms of the National Instruction 1 of 2008 and with the condition that the researcher provides a copy of the research report to the Directorate for Priority Crime Investigation (DPCI). The researcher used this letter as a means to access the Divisions or units of the SAPS to conduct research and recruit participants. After gaining access to participants, the researcher had to endorse informed consent.

4.16.2 Informed Consent

In research involving human subjects, informed consent is an essential concept that protects the participants' well-being (Mandal & Parija, 2014). Informed consent aims to give participants easily understandable information about the study so that they can decide whether or not to participate. Usually, it takes the form of signed contracts that specify the study's goals, benefits, risks, and other pertinent information. All participant communications must adhere to informed consent guidelines. It is the researcher's duty to advise participants of any dangers and potential benefits of the study. Following receipt of the given information, participants must voluntarily offer their consent (Nijhawan, Janodia, Muddukrishna, Bhat, Bairy, Udupa & Musmade, 2013). Research consent needs to be genuine, comprehensive, and transparent. In the event that participants are minors, permission from parents or guardians is required (Mandal & Parija, 2014). In this study none of the participants were underage.

Before the interviews were conducted, the researcher obtained informed consent from the participants. different steps were followed to ensure that the participants are well informed about the study. Firstly, the participants were given a written agreement to sign and indicate their willingness to participate in the study. The researcher ensured that the written agreement included detailed information about the study and allowed participants to fully comprehend it before they decided to participate in the study.

The informed consent included the following components to inform participants' decisions:

(a) The topic of study.

(b) The purpose of the study

(c) The duration of the interview.

(d) Risk or discomfort-there was no anticipated risk associated with the study and the participants did not experience any risk

(e) The study had no compensation to participate in the study.

(f) Declaration of confidentiality was also mentioned, including a description of who may access interview records, how their personal information will be protected, and how recordings will be kept safe.

(g) The researcher's details were included for any questions or queries related to the research.

(h) and lastly, participation was voluntary, and refusal to participate or discontinuing participation at any time will not involve any penalty or loss.

The researcher ensured that the participants willingly signed the consent form. For instance, the researcher did not use any intimidation or demands when administering the informed consent. The participants were informed verbally and in writing of all the data collection methods and activities that will be conducted. Voluntary participation was also parament.

4.16.3 Voluntary Participation

The term volunteering is widely used in research ethics but rarely well understood. Kılınç & Fırat (2017) define voluntary participation as a decision and action made independently of other people or influenced by external sources. Participation was solely voluntary in this study, and participants were informed of their rights to choose whether to engage or not in the study. There were no compensation or reward benefits, and participants were informed that it was for the benefit of the public, knowledge contribution, the benefits of the South African economy, and contribution to research. All 17 participants were willing to participate and consented to engage with the researcher.

4.16.4 Confidentiality, Anonymity and Privacy

For participants, confidentiality and anonymity standards are essential in research. These ethical standards promote honesty and trust, which has a beneficial effect on collecting data. Study participants must be assured of their privacy and anonymity to avoid harm. Because study outcomes are more valuable to researchers than participants, researchers must respect confidentiality and anonymity standards to preserve participants' privacy (Kang & Hwang, 2023). Confidentiality violations can result in financial difficulties, social humiliation, and shame. For studies to be effective, researchers and participants must build rapport and trust. Rapport and trust with participants can only be achieved through openness and transparency. The quickest and easiest method to build a relationship of believable trustworthiness between researchers and subjects is to protect subjects' right to privacy through excellent confidentiality and anonymity measures. Should these guidelines not be adhered to, the study might not be accepted or regarded as trustworthy. Integrity may only be attained by providing informed consent information (Kang & Hwang, 2023).

The researcher ensured that confidentiality was maintained throughout the whole research process. Participants were given the privilege to stay anonymous throughout the study. Since this study used tape recorders during the interview phase, the participants were informed that their responses were being recorded. When recordings were transcribed, the researcher employed pseudonyms to ensure participants' confidentiality. Once their responses and information have been obtained and analyzed, the recordings will eventually be destroyed or deleted from the recording device.

4.17 Data Storage

Data collection, protection, and management are the researcher's responsibility. After transcription, all recorded data should be deleted and destroyed to protect participants. The data should have a secure storage system if the study is incomplete (Alase, 2017). To protect the participants, the researcher ensured that the recordings were placed in a protected file or folder and required a password to access them. The researcher only knows the password. The recordings were also uploaded on a personal Cloud drive to avoid loss of the recordings before the study was completed.

4.18 Limitations of the Study

Limitations are difficulties that researchers encounter, many of which are out of their control and might have an impact on the findings and interpretations of the study. No matter how good a study is or how carefully planned or executed, all studies have some restrictions (Akanle, Ademuson & Shittu, 2020). The researcher understands that there are limitations to everyone's work; however, to increase the research's credibility, efforts must be made to overcome these obstacles. The challenges the researcher encountered in the investigation are listed below.

4.18.1 Participation in the study

The researcher faced a few challenges while conducting the study. These issues came from the participant's reluctance to participate in the study. There were challenges with gaining the trust of the police officers, especially the issue of questioning and electronic recording of responses. The researcher seemed to have underestimated their reluctance to participate. However, it was also understandable due to the nature of their work; they could not afford to overly trust a

stranger. Their jobs sometimes required them to investigate even their own colleagues and very trusted and high-ranking members of the police force. Therefore, it was not surprising that they doubted or appeared circumspect of the intentions of the researcher. Building trust was imperative. The researcher had to assure them that the study was for academic purposes and that their personal details would be kept confidential. The researcher explained to them she was under an obligation not to break their trust or be unethical.

They were given consent forms; and briefed on the purpose of the study, emphasizing that their participation was voluntary and would be a big contribution to the research. This part of the study required that the researcher demonstrate good communication skills and demeanor. The briefing was conducted in a very warm and friendly manner, which made the participants feel at ease and give their consent. All the participants voluntarily agreed to be recorded.

4.18.2 Data Collection and Time Constraints

Although participants agreed to participate in the study, having time to interview them was a bit challenging. Their duties required them to be constantly in court and investigating cases. The researcher had to be flexible in accessing the participants and working around their busy schedules. The researcher had to exercise patience and be very understanding in this instance. The participants agreed to an appointment; however, they sometimes rescheduled another time due to urgent matters that they had to attend to. Others would be disturbed during the interview, and the researcher would have to wait a few minutes. This caused the collection of data and/or interviews to take longer than anticipated.

4.18.3 Limited Sample

The researcher had planned to conduct interviews with 25 participants. However, only 17 participants were available and interviewed in the study. The researcher needed to interview participants who had knowledge and experience in the field of cybercrimes. Therefore, the researcher interviewed 17 participants with rich knowledge rather than focusing on fulfilling the anticipated number and interviewing participants with just limited and general knowledge of the field.

4.19 CONCLUSION

A research methodology was discussed in this chapter. The study adopted the interpretative paradigm. This paradigm seeks meaning and examines the complexity of the human world's subjective experience and social reality. This paradigm is appropriate in qualitative research studies and seeks to find subjective meanings. Therefore, the qualitative approach was the most suitable for answering the study's research questions. It sought subjective opinions or views of the participants on cybercrimes. The explorative research design was adopted. Exploratory research is suitable when there is little prior knowledge or insight into a subject and when the objective is to produce ideas and insights that can direct further investigation. There is limited knowledge about how South Africa (or SAPS) combats cybercrime and whether it has been successful. The study wanted to discover and add new knowledge, therefore exploring the study under investigation. The population included the South African Police Services (SAPS) and a sample of 17 participants, all of whom are experts in the field of online crimes. The study adopted a purposive sampling strategy to determine who should be included in the study.

Data was collected in the form of semi-structured interviews. Interviews were considered appropriate for this research because they consider flexibility and allow participants to speak freely, allowing the researcher to obtain all the information relevant to the research questions. An interview schedule was developed to guide the interviews. Thematic analysis was conducted to describe and interpret participants' views and analyze data. Ethical considerations were also discussed in the study. Informed consent forms were used to inform the participants of the purpose of the investigation, protect the participants, and give them an opportunity to decide whether or not to participate. Participation was solely voluntary in this study. The researcher further respected confidentiality and anonymity standards to preserve participants' privacy. The researcher also encountered some challenges during the study, including sample size, time constraints, and endorsing participants to participate.

CHAPTER FIVE

DATA PRESENTATION AND INTERPRETATION OF FINDINGS

5.1 Introduction

This chapter focuses on data presentation and analysis of the findings of the study. The study aimed to explore the South African Police Service's (SAPS) system for combatting cybercrime and if they are effective. If ineffective, how can the systems or approach be enhanced to ensure cybersecurity or online safety and maximize the benefits of the digital revolution. The key research questions were as follows:

(i) What systems or approaches are currently implemented by SAPS to curb cybercrime?
(ii) How effective are the existing SAPS systems in responding to cybercrimes?
(iii) What types of cybercrimes do SAPS encounter?
(iv) What are some of the challenges SAPS encounters when dealing with cybercrimes?
(v) What interventions can be recommended for SAPS to adopt to curb cybercrime effectively in South Africa?

To begin with, it may be worth noting that to uphold ethical standards, the presentation of the data and analysis does not reveal the participants' real names. Instead, they are identified as P1-P17, with P representing the participant. The study's objectives guided the identification of the main themes, while the sub-themes were derived from the interview schedule. Lastly, concluding remarks are given at the end of the chapter.

Table 5.1 **Illustration of Theme Development**

Themes	Sub-Themes	Categories/Subtopics
To explore the Systems currently employed by SAPS to curb cyber-crime.	-The Roles of the South African Police Officers in the DPCI and Commercial Crimes Unit -Police Officers Views on Cybercrimes in South Africa	

	-Procedures used by SAPS to respond to Cybercrimes	
To determine the effectiveness of SAPS systems in responding to cybercrimes	- The effectiveness of SAPS in decreasing, responding to, or convicting cybercriminals in South Africa. - Job Satisfaction	
To investigate the Types of Cybercrime that SAPS encounters	-The Types of cybercrimes that SAPS encounters in their line of duty.	Hacking Ransomware/Cyber Extortion Identity Theft and Online Fraud Scams/Scammers Phishing Attacks
To examine the Challenges (if any) that SAPS encounters in dealing with cybercrimes	-The Causes of Cybercrimes -Challenges that SAPS encounters when dealing with cybercrimes	Lack of Skills and Inadequate Capacity Time constraints Corruption Underreporting Jurisdiction Issues and Mutual Agreements
To recommend interventions that SAPS can adopt to curb cybercrime	SAPS perceptions on interventions to improve their capability to effectively decrease or respond to cybercrimes -Perceptions of SAPS on how the public can protect themselves from cybercrimes	

5.2 Systems Currently Employed by SAPS to Curb Cybercrime

This theme sought to understand the ways in which police officers respond to cybercrimes. The researcher first determined the roles of participants and understanding of cybercrimes, which was an essential factor in the study and in responding to the phenomenon under study.

5.2.1 The Roles of the South African Police Officers in the DPCI and Commercial Crimes Unit

The participants interviewed seemed to understand their roles in the SAPS cybercrime department or unit. Asked about how they understood their roles in the cybercrime unit, the participants responded as follows:

P1: "I am digital forensic investigator. My role is to extract, process, and analyse digital devices"

P2: "I am an investigator, mostly dealing with banking-related issues. Anything related to asset finance to cybercrimes"

P5: "I work as a forensic investigator for SAPS, Commercial Crimes Unit. I deal with dockets that encompass cybercrimes. That is my specialty. I found it interesting and challenging at the same time. I can be able to see and find links within the dockets"

The study's findings revealed that police officers in the SAPS cyber unit understood their roles and were experts in their fields. They showed they had the ability and skill to respond to online crimes. The findings confirms expectations, as observed in much of the literature. The staff of Forensic units globally must have information technology and computer forensic skills for forensic analysis of electronic evidence and be able to successfully investigate and prosecute cyber offenders (Van Vuuren et al., 2020). Having an expert involved in the cybercrime case ensures that no fabrication of evidence and data collected is rendered as inadequate evidence in a court of law (Kempen, 2019).

Other participants played specialized roles, focusing on, for instance, fraud and/or internet fraud as they dealt with cybercrimes in the financial sector (such as the banks).

P6: "I am a fraud investigator, but am not limited to fraud"

P4: "I am an investigating officer investigating banking fraud cases and cybercrimes"
P9: "I am an investigator. I investigate banking crimes, which include internet fraud, asset finance, and scams"

The roles of these investigators further depicted that cybercrime in South Africa is also more financially related and, therefore, requires expert personnel in that field. This also indicates that police officers do not only need to protect the public but must consistently protect the country's economy as a whole. SAPS recognizes the need to provide all South Africans with a safe and secure information technology environment (Kempen, 2019). By having these units, SAPS further addresses their constitutional obligation to adopt measures, policies, and/or strategies to deal with cybercrime. In the context of the Routine Activities Theory (RAT), the "guardians/guardianship" of cyberspace is present, and police forensic experts (under SAPS) prevent and respond to cybercrimes (Li, 2018).

5.2.2 Police officers Views on Cybercrimes in South Africa

It was evident that the common perspective for all interviewed participants is that cybercrimes are on the rise in South Africa. The participants supported their arguments, reflecting on Cybercrimes in South Africa as follows:

P3: "Cybercrime is increasing. We try to combat it, but for now, it's not enough because, as a country, we are not up to standard regarding cyber-related issues. For example, technology in South Africa is being phased In, and everyone now has a computer, but when it comes to knowledge, we are not up to standard yet. People carry iPhones but are not sure how to use them. In America, they carry iPhones, know them, and are technically savvy. So, they can commit crimes against you because you do not know the capability of technology. So that gap leads to more cybercrime"

P1: "Cybercrimes are increasing; the reason is that in South Africa, we are backward, unlike other countries, like the US, where they have been exposed to technology for a long time. In South Africa, we were not that exposed until recently. Even Nigeria is more exposed to technology, and even their Data is cheaper because having access to the internet requires data."

P10: "South Africa is at its highest peak of Cybercrime, and because people don't understand what cybercrime is, we are mostly targeted. Everything goes electronically via phones and emails, and it's much easier to commit crimes with these gadgets."

P12: "Cybercrime in South Africa is not properly managed, not because the government does want to decrease crime but because we are behind when it comes to cyber-related stuff; we are still catching up. While the people who commit cybercrime are ahead."

Participants' views demonstrated that the increase in cybercrimes was caused by the fact that many South Africans are still not advanced in cyber technology and unaware of online crimes and their severity. Evidently, the country is developing fast in technology, which is beneficial, although it also comes with disadvantages, an issue widely acknowledged in the literature. Barret (2013), for instance, contends that the challenge with the increase in internet use is the exposure of many people to the risks of cybercrime. Unfortunately, many people are unaware of the risks or how to protect themselves from cybercrimes. Invariably, cybercriminals target the unprepared, who easily fall prey to the dangers of online crimes.

Other participants shared their views as follows:

P13: "Cybercrimes are definitely on the rise. Ever since, technology has become more advanced and gained popularity in South Africa. The hackers have used that to their advantage. Although technology has advantages for the general public, it also has benefits for crimes"

P16: "Well, currently, it is the leading way criminals are getting money. If I'm not mistaken, South Africa is number 6 (Six) on the list for the most cybercrimes in the world. We are behind a developed country like America; in Africa, we are the third (3) in cybercrimes. Cybercrime in South Africa is a major problem. And we are going to get worse. In no time, cybercrime is going to be the number in which crime is committed"

P8: Cybercrime in South Africa is not properly managed, not because the government does not want to decrease crime but because we are behind when it comes to cyber-related stuff; we are still catching up. while the people who commit cybercrime are ahead.

Mabunda (2021) supports the participant's views and stated that South Africa is one of the African countries that currently faces a major challenge regarding cybercrime. The development of technology and more people using the internet has invariably spawned increased cybercrimes. Masthead (2020) also claims that South Africa ranks third globally in terms of cybercrime victims. In relation to RAT, Olayemi (2014) asserts that daily computer and internet activities, legal or illegal, place individuals in closer proximity to motivated offenders. This is inevitable as many people utilize the internet and spend a lot of time online. Mabaso (2018) states that about five billion people are connected in cyberspace, with almost 50 billion technological devices being adopted, and Criminals are exploiting this connectivity. The public utilizes technology in school, work, or home. The growing internet connection makes it easier for cybercriminals to carry out their illicit activities. The internet allows cybercriminals to swiftly and inexpensively send many emails (Phishing) to a worldwide pool (Baylon & Antwi-Boasiako,2017).

Other participants also believed that cybercrimes are on the rise in South Africa and that law enforcement officers require consistent training. They also argued that technology was developing fast, and criminals were always far ahead of law enforcers. Thus, cybercrimes tend to increase as the rate of change in technology also increases. This is what some of the participants had to say:

P17: "Cybercrimes Are definitely on the rise. Criminals are getting so technologically advanced, even we ourselves need that specialized training to keep up"

P6: "Cybercrimes are on the rise, and most police officers do not have the skills to investigate it."

Mugisha (2019) and Wu, Breitinger, and O'Shaughnessy (2020) posit that cybercriminals can defraud anyone in the world and possibly evade detection. This means that investigators need to keep up with the pace at which the speed of technology is developing. They have to develop and acquire new ways of responding and apprehending cybercriminals. From the structural functionalist theory perspective, all this is occurring as a result of structural failure, which makes bringing about stability in cyberspace a challenge for law enforcement officers (Rustad, 2001). The police officers struggle to keep up with the pace of the growth and advancement of technological systems.

5.2.3 Procedures used by SAPS to respond to Cybercrimes

According to Mabunda (2021), African Countries have introduced strategies and security laws to prevent cybercrimes. Reddy (2019) state that The South African government is required by the cybercrimes bill's Chapter 10, Section 54, to ensure that the member of the Cabinet in charge of law enforcement must provide a sufficient human and operational capacity to detect, prevent, and investigate cybercrimes.

In this research study it was revealed that although participants were in the same line of work and investigating cybercrimes, their roles in responding to cybercrimes in the department differed a little bit. They have digital forensic investigators who deal with extracting evidence from digital devices (Computers, phones, etc.). They also have investigators or forensic investigators who go into the field, investigate the cases, link evidence received from digital forensic investigators, and build a case against the offender.

In responding to cybercrimes, digital forensic investigators Stated:

P1: "We usually receive a request, and then we do the extraction of evidence. We then send it back to another investigator. The investigator will check if the evidence correlates with their desire. The forensic investigator has to make a link depending on what he wants and to whom does he wants to prove or link it. I also need to submit a statement that I am the one who gave the evidence and confirm that I am the expert on it. I did not temper with any data; it is the original or mirror image of the original content. We create a report of what we did to collect evidence, and at the court, we present it as an expert. For example, they will give us a cell phone and they will know what they are looking for. Maybe they want to see WhatsApp messages, so we do the extraction of all the messages, even the deleted ones, and the investigator reads them and analyzes that evidence. Once they compare the evidence, they come back to the digital forensic investigator to say can you write a statement for us based on what we have seen or found from the extracted data. At court, the digital forensic investigator will testify that they exhibited the evidence from the suspect."

P4: "As a digital forensic investigator. We receive the laptop or computer equipment, and we have to access any data that is there and analyse it."

P6: "There is technology and some software that we use to assess and detect who and how the crime was committed. How they were able to access your email we are able to see that. Criminals use online systems; they use keywords of any money, payout, or transaction that was made by the user. Those keywords would go to the criminal activity, and they can just change it and use it against the user"

Wu et al. (2020) note that more practical rather than theoretical measures are needed to combat these crimes. The study revealed that digital forensic experts are important in detecting and investigating cybercrimes. The fact that the researcher was able to find and interview these experts shows that law enforcement authorities and governments have established cybersecurity and digital forensics units to investigate cyber incidents. These experts possess the necessary information technology and computer forensic skills to investigate and capture cybercriminals (Mugisha, 2019 & Wu, Breitinger & O'Shaughnessy, 2020). Reddy (2019) states that digital forensics ensures the successful prosecution of cyber offenders and further ensures that there is no fabrication of evidence, and that data collected cannot be rendered as inadequate evidence. Van Vuuren et al. (2020) further support this study and state that the experts' skills are needed for the forensic analysis of electronic evidence and a successful investigation and prosecution of cyber offenders.

Digital forensic experts are important because digital devices used by the offender or the victim increasingly contain evidence of many kinds of crimes (such as fraud, drug selling, human trafficking, assault, and murder). Digital traces are left by every action taken on a person's computer system and a business network. These traces can be anything from cookies and web browser history caches to document metadata, erased file fragments, email headers, and more (Mugisha, 2019).

Investigators or forensic investigators in responding to cybercrimes commented as follows:

P2: "There are forensic investigators that we refer to and get IP addresses. so they can extract information we can use to search for evidence. We would use Section 205 as a subpoena. We would subpoena internet providers such as Vodacom or whichever service provider was used while committing the crime. Section 205 allows access to confidential information. If R200 000 from my victim's account was stolen, I want to see who received it. So, we will order that bank to give me that person's bank account details or statements. You can also subpoena any other people that might be useful in the case."

P3: "Someone would first come to report that they have been victimized. For example, someone would come to report that they have lost money from their bank account, but they did not make any transaction. We need to get permission from the magistrate, which we call section 205 subpoenas, to get information. It could be your information as a perpetrator or your information as a victim."

P7: "A docket must be registered before we investigate or get information. With a docket opened, we are able to use section 205 and compel certain entities to give us information to use in our dockets for court processes."

Police officers must gather evidence to prove that crime has occurred and prosecute offenders. Al-Dhaqm, Ikuesan, Kebande, Razak, Grispos, Choo, Al-rimy and Alsewari (2021) state that for criminals to be prosecuted, scientific evidence that is reliable and relevant to crime must be collected and submitted to the court of law. Without scientific evidence, it is quite impossible to link a potential offender to a cybercrime incident. This theme revealed that the first responder needs the right authorization, such as consent or a court order, to look for and gather evidence at an electronic crime scene. To obtain evidence, the first responder needs to be able to determine the legal justification for doing so (Mugisha 2019).

Furthermore, the government of South Africa has taken steps to enact various cybercrime laws and/or legislation (Gumbi, 2018). The participants mentioned Section 205, of the Criminal Procedure Act 51 of 1977, which they often use, with the assistance of the courts, to subpoena witnesses (e.g., service providers, banks, offenders, etc.) for interrogation. This procedure, in most cases, enables them to have access to very useful confidential information. Receiving permission from the court meant that officers could quickly investigate the crime and would not have to wait long or put their investigations on hold. The process is in line with Reddy (2019) who draws attention to Section 31 (1) of the cybercrimes bill, which allows a police officer or investigator to request technological support from electronic service providers, financial institutions, and individuals in order to locate, access, or seize an object. The laws, thus, provide the necessary support investigators need in their efforts to promptly identify criminal activity, gather intelligence and evidence, and analyse evidence that has been retrieved.

Participants 13 and 15 commented and mentioned the impact that borderless crimes have in their investigations and responses to cybercrimes:

P13: "Firstly, as an investigator, I need to establish where the crime took place; say you have received an email, and you have responded to it. The main thing we would do is get the IP address and figure out where the emails were sent from. Once we have the IP address, we will subpoena the bank accounts and see where the money was transferred or withdrawn. So, we follow the money trail. Some criminals like to buy expensive clothes and cars, so we follow that up and their accounts, especially if they buy in one place more often. we can get cameras and maybe descriptions of the suspect. Sometimes, they would even know who that person is, and we will follow that up and eventually arrest the suspect

The only challenge is that the emails could come anywhere in the world; you might think it's from SA, only to find it's from America. That becomes difficult to investigate because we must go through Interpol, so we must accommodate the policies there. It has become difficult to investigate or prosecute those criminals. Most cyber offenders also come from Nigeria, operating everywhere from Europe to America. They have people everywhere around the countries"

P15: "In one of the cases I was involved in, we had to get mutual assistance from abroad, and that is always difficult, especially if they do not cooperate. Also, our digital team had to assist with the extraction of evidence from the devices."

The participants' responses revealed that international collaboration is sometimes required to investigate and respond to cybercrimes. Hofmeyr (2020) mentions that Cybercrime has evolved into a global issue that requires an international response. Section 3 of the Cybercrimes Bill guards' crimes committed outside South Africa. These crimes are trailed if they affect the Republic of South Africa. Crimes related to Cryptocurrencies are examples of crimes that cross jurisdictions (Reddy, 2019). Chapter 6 of the Bill, in conjunction with Chapter 2 of the International Co-operation in Criminal Matters Act of 1996, offers reciprocal support for investigation of cybercrimes and evidence preservation. However, Wang, Hsieh, Chang, Jiang, and Dallier (2020) state in support of the participant's views that there are still challenges in fighting cybercrime. There are issues with jurisdictions and receiving support from the various authorities of the countries that are affected by cybercrimes. This causes delays and insufficient progress in receiving clearance for the investigation of cases.

Participant 17 considered creating awareness of cybercrimes as another means of responding to cybercrimes.

P17: "What we try to do is to make people aware of these crimes. We have been broadcasting awareness campaigns between us and the banks that people must not give out their personal information. But these people target the elderly and people in rural areas who don't know much about technology. So, the best thing we can do is make people aware of it, then more people will be able to be careful and avoid scams"

From the above response, it is evident that police officers also have to collaborate with companies within the country to decrease cybercrimes. Gumbi (2018) states that police officers encounter victims of different types of cybercrime attacks (such as identity theft and online fraud). To respond to these crimes, they must collaborate with private companies (such as commercial banks, security companies, internet Providers, etc). The police must strengthen their relationship with banks and security companies and collaborate in organizing awareness campaigns such as conferences and workshops. The police must further develop a means of continuous contact with internet service providers to ensure they are aware of any changes being made that could affect cybersecurity systems. Undeniably, this theme revealed that there are units or departments in South Africa that deal specifically with cybercrimes and are in line with the constitutional obligation to adopt and address the measures, policies, and/or strategies developed to deal with cybercrime. These units under SAPS are, namely, local police stations, the Commercial Crimes Unit, and the Directorate for Priority Crime Investigation (DPCI, also known as the Hawks). Others are the Special Investigating Unit (SIU) and the National Prosecuting Authority (NPA).

The functionalist school (Structural functionalism theory) asserts that social structures fulfill specific demands and that functional imperatives must be met for a community to survive. In other words, society must have balance to survive and function. Cohesive integration will result in the society being perceived as a functionally integrated system and in a state of balance. The theory, therefore, views society as a collection of interconnected and interdependent social structures (Pasaribu, 2018 & Enweonwu, Ugwu, Onyejegbu, Areh & Ajah, 2021). In this instance, laws must be communicated and shared for effective implementation and investigation.

5.3 Effectiveness of SAPS systems in responding to cybercrimes

This study revealed that there are police experts who can respond to cybercrimes. Therefore, this theme aimed to understand the extent to which SAPS have succeeded in their investigations of decreasing and/or responding to cybercrimes.

5.3.1 The effectiveness of SAPS in decreasing, responding to, or convicting cybercriminals in South Africa

Kempen (2019) argues that the role of the SAPS or state to combat cybercrimes effectively is still questionable. Most participants seemed to agree that they have not been quite successful in dealing with cybercrimes, which they attribute to the lack of expertise in the field, while other participants mention a lack of capacity in the field.

Some police officers indicated that they have had some degree of success and stated:

P2: "To a great extent, we have been effective because in most cases that come here, we need us when we go to court; the court does not even argue with our evidence. because we have proven it is the original and taken from the suspect device."

P8: "We had a case some time ago where a lady was arrested for cybercrime of hacking. Through banks and SABRIC, we were able to arrest her because we work a lot with SABRIC as well. So, we used a cell phone to track her and finally made an arrest. She was sentenced to 3 years imprisonment. The other two guys we had arrested for fraud, their sentence went up to 20 years. Some offenders do receive a suspended sentence. Each case has its own merit."

P9: "In the past, we haven't been successful; it is only now that we have recently opened a unit that specifically investigates cybercrimes. In the other provinces, like the eastern cape, they have also recently opened their own unit."

These participants based their claims on their ability to prove to the courts that the evidence submitted was valid and adequate. They also attributed their successful convictions to technical

support by the state and improvement in their capacity to deal with cybercrimes, which implied that with the support of their political principals, the forensic unit can be very productive.

The courts can also play their part. Boda et al. (2021) state that the bill allows for extensive penalties that could be imposed on anyone found guilty of cybercrime. A court will have the discretion to impose a penalty that it thinks is suitable under Section 276 of the Criminal Procedure Act 51 of 1977. An offender could either receive a fine or imprisonment for five to ten years. An offender may also receive a maximum of 15 years in imprisonment for aggravated offences, which could serve as a deterrent.

Other participants commented on their shortfall and limited capability and challenges they face when investigating cybercrimes:

P10: "Not to a great extent because we are dealing with faceless people, and before even getting to them, you need to apply for permission in court, and it is even more difficult when you find that the location of the perpetrator is someone who is far or overseas."

P12: "We try, but I can say we have not really been successful; it is even hard to estimate the progress we have made in dealing with cybercrimes. And I think it is because just a few of us know how to investigate cybercrimes. It is difficult because most of the police force, they do not have the necessary training in this. We have a unit here that has to assist the whole of kzn with cybercrime cases. There are not many of us."

P11: "SAPS has the cybercrimes unit. Unfortunately, the cybercrimes unit is in its infancy stages and under-capacity to deal with cybercrimes on a macro level. With the number of cases coming up now, SAPS is not capable of handling these cases. We also do not have properly trained members to investigate these crimes. They are, however, in the process of increasing the capacity, but as we stand, we still lack capacity.

So, our success is minimal, 5 to 10%; I stand to be corrected. There are some convictions, but they are not many."

The police officers asserted that they were unsuccessful at times because of the long process that had to be followed in their investigations. They were further challenged by the limited capacity in terms of human resources relative to the increasing number of cases to investigate**.** Evidently**,** as Baylon and Antwi-Boasiako (2017) assert, cybercrime laws are often poorly enforced, and prosecution also becomes more challenging due to the high number of victims who reside in other countries and not in the same country as offenders. Cybercrime investigation units are short-staffed and lack adequate training.

The following responses also highlighted the problems experienced in dealing with cybercrimes:

P5: "It all depends on the circumstance. Cybercrime is very difficult to investigate because it happens anywhere in the world and by anyone. You might not even be aware of it until it has been done. Sometimes, it can take months to see that you have been a cybercrime target. And everything would have been erased at that. We have had successes in which we have managed to convict people. Unfortunately, in some cases, we only become aware of it six months later, and we won't have access to most of the evidence we would have collected. We will then not be able to proceed with the case any further. So, at present, probably 30% successful with the cases."

Participant 14 Responded as follows:

P14: "Once a crime is committed, we must act fast; we can't wait too long. Criminals mostly use a device only for a short period, so you must act fast and report that crime."

With these challenges, the tendency to commit cybercrime continues to escalate because few perpetrators of these crimes face penalties or legal retribution. Świątkowska (2020) argues that the internet is designed in a way that provides anonymity, allowing criminals to operate behind several layers of false identities and encouraging covert activity without being arrested. The digital environment poses difficulties for even the most basic processes, such as gathering, preserving, and assessing evidence. There is a need for highly developed technological expertise to face the reality and challenges associated with cybercrimes.

5.3.2 Job Satisfaction

This question was an extension of the above sub-theme, and the objective was to understand further the participant's views on their profession in dealing with online crimes. Some of the interviewed participants portrayed their jobs in a positive light and acknowledged that their profession had a positive impact on society. They perceived challenges as part of their profession, which they had to and were often able to deal with successfully.

Participants 1,4 and 5 reflected in their responses:

P1: "It has improved my satisfaction because I am doing something that counts. We encounter advanced criminals who commit these crimes, and we are an opposing force against them. And if we were not here, there would be more of them, and they would take advantage of the country.

So, we are pushing back. As I said, the country is backward, so I feel as though I am one of the few who are pushing forward and dealing with these crimes."

P4: "We get satisfaction when we get a good sentence or an arrest. It is even more satisfying when a victim gets their money back. We have cases like that where victims are compensated."

P5: "So far, we know that we have to serve you, and we do not give up even if we do not find them quickly. We still follow them."

Their positivity seemed to come from their satisfaction when they could convict or arrest these criminals and when victims were compensated for their pain and loss. Their focus is on serving the South African public as they have sworn and committed themselves, regardless of the challenges or circumstances they experience. Participant 10 also declared:

P6: "Sometimes you see that people are being defrauded and defrauded of their entire life savings. And our department may take a minimum of two years to investigate this. So, it takes a long time to finalize a case, but at the end of the day, knowing and arresting these criminals is the most satisfying feeling. It drives you to continue; no matter how long it takes, we want justice to be served."

This comment further revealed that no matter the circumstances, consistency, patience, and focus are important in their investigations (or responding to cybercrimes). What is important is the end goal, which is to convict these offenders. That brings satisfaction, positive energy, and encouragement to police officials. They understand that they have to uphold the level of responsibility and live up to the expectations of the public, especially victims.

Participants 11 and 8 commented:

P11: "It's a learning curve every day"

P8: "Cybercrime is an interesting area to engage in, we learn new things daily. And it is quite interesting how cybercriminals are always looking for new ways to offend and crack systems. So, it is interesting but also challenging."

They considered their line of work as an interesting area that wanted them to learn and evolve. Indeed, Cyber-offenders always find creative ways of offending and targeting the public. Therefore, it is important that police officers continue to improve their prevention strategies to curb cybercrimes (Boda, Dullabh & Steele, 2021).

Other participants reported that although they like their jobs, they are concerned with the conditions of their work and the nature of these crimes. They mentioned work overload, insufficient training, funding, etc.

Their responses were reflected as follows:

P13: "I have so many files, and it is difficult to give a single case 100%, but when you finalize it, your hard work pays off. So that is what drives me. Also, we have what we call asset forfeiture, so all assets that were ceased from the offender may be given back to the victim. But in most cases, cybercriminals use the money immediately, and there is nothing left."

P16: "It is a challenge, all these interdicts, organizations, banks, they change their products all the time. You find that as we investigate, they have these new products on the market, and certain products have changed, but we do not get efficient training and updates on these products. And providing training all the time as these new products emerge is time-consuming and expensive."

P17: "It's quite frustrating, and it's going to get a lot worse as years go. We want to solve these cases, but we need more training, and it should start at the college level. we need to train the younger generation to deal with these crimes. We need to educate younger policemen because here we are old now. The more people we train the easier it would be to combat cybercrimes. We need experts from outside of South Africa as well to train the police who investigate cybercrimes"

With the 4IR development, the necessary skills are essential for digital safety and security. Both formal and informal education are required. The educational system must provide cybersecurity courses or research projects. This is especially important in developing nations where knowledge of information security is still lacking and is not contingent on fluency in English. Participants revealed positive and negative aspects in their line of work. However, it was important that they always tried their best to respond to these crimes. The aim is to protect, bring back hope to the victimized, and get the criminals out of the street and space where they can defraud and harm others. It did not matter how long it would take them.

5.4 Types of Cybercrime that SAPS Encounters in their Line of Work

Participants highlighted several online crimes, such as identity theft, phishing, hacking, ransomware, and online fraud, and considered these crimes as the most prevalent. Hjertstedt (2019) states that Cybercrime happens in various ways and on various internet services.

Any crime committed using online services can be regarded as cybercrime.

Participants responses were as follows regarding the types of cybercrimes:

5.4.1 Hacking

Hacking was mentioned by participants 2,5, 17, and 6 as being one of the prevalent crimes they encounter.

P2: "Usually, it is hacking, where they hack somebody's account and redirect funds to fraudulent accounts that have been opened. For instance, if you are buying a house from the bank, they will send you banking details via email. You find that an offender using the same bank will just make little changes that you will not notice. So, when you send funds, you won't be able to see that you are no longer using the correct banking information."

P5: "A lot of individuals or syndicates hack into emails and change email addresses, get new pins, and transact money using those details"

P17: "We would come across hacking. for instance, there was one company that had ordered some goods overseas, and they were liaising via email. Someone hacked their emails. Both South African and overseas companies were still under the impression that they were liaising with each other. However, this person was monitoring their communication and when they sent their banking details so that the South African company could pay for the goods, these criminals changed the bank details so that the money could be deposited directly to them"

P6: "Another new one is when they are hacking the emails and changing bank numbers, and then the money would be transferred to the suspect account. for example, we had an attorney's system being hacked and his clients were given the wrong bank account to pay to, and money was paid to the suspect account another"

Joynt (2023) considers hacking as "cunning" methods used to gain unauthorized access, interfering with, or intercepting data by using "smart" network techniques. Criminals use harmful malware to obtain more by stealing sensitive data and passwords or by taking advantage of victims. These criminals can gain access to electronic information such as stealing sensitive data and passwords from banks, transferring money to a third-party account, and buying expensive items in the victim's name (Shola, 2021 & Saweneh, 2020). When cybercriminals gain access to your computer it leads to your identity being stolen and can have significant financial and reputational loss.

Participant 13 stated:

P13: "We have come to understand that most cybercrimes are financial in nature. hackers are hacking to gain money. They hack individuals' emails and companies. What they do is they put keylogger software to companies' networks and hack the network or block the company from trading. They hold the companies at ransom and would want the companies to release or pay an amount of money before they can unblock the system. They take over the ownership of your accounts, where you cannot order or receive orders from a company. So, they can claim huge sums of money. It is an international practice, and the worst-case scenario is when the hacker is not even in South Africa or in that country they are defrauding"

This is, in fact, part of ransomware, where a hacker encrypts data and restricts access (Kagita, Thilakarathne, Gadekallu, Maddikunta & Singh 2020). After encrypting the victim's data, the hacker will require payments in order to release the system. It can have a major effect on a company and a country's economy.

5.4.2 Ransomware/Cyber Extortion

Indeed, the study revealed that ransomware and/or cyber-extortion were also a challenge in South Africa. Participant 15 responded:

P15: "We all also have the business takeovers, where someone will access the business computer and steal all their information and use that to ransom you to pay a certain amount of money to get that information back. So those are the most common here in South Africa"

This is a classic case of cyber extortion described in the literature. Nnaemeka (2023) and Sawaneh (2020), for example, explain that Cyber extortion is the result of persistent denial of service by malicious cyber criminals on a website, email server, or computer device. It involves the stealing of confidential data and the threat of exposing it to the public in return for money to avert or terminate the attack. It is comparable to ransomware attacks in which cybercriminals demand money in exchange for a promise to either stop the assault or offer protection.

5.4.3 Identity Theft and Online Fraud

The literature shows that in South Africa, identity theft is common and fuelled by growing internet connectivity, corruption, and challenges in obtaining a conviction (Hjertstedt, 2019). True to expectation, some of the participants mentioned this cybercrime.

One of the participants (P4) said, "*We get a lot of internet fraud that includes asset finance such as*

loans, where they use and send false payslips or bank statements to be approved for loans."

Another participant said, *"Usually, it is identity theft or fraud where they will take your password and usernames that would be used to steal information and money. They also steal your social media profile to advertise some products such as forex trading." (P 11)*

Identity theft involves unlawfully attaining someone else's bank accounts or personal details, with the aim of making unauthorized transactions or purchases (Joynt, 2023). Offenders may steal personal information such as date of birth, house address, name, password, email, etc., to apply for loans and create fake social media accounts. Cyber offenders may use the stolen identity to open accounts and buy big-tickets or items. The crime can occur from either alive or deceased individual. The number of social media identity thefts is also rising (Chudasama, Patel, Shah and Shaikh, 2020 and Sawaneh, 2020).

According to Younes (2019), there is an increase in online fraud, which involves tricking people into giving up crucial account information, stealing their money, espionage, or impersonation. They sometimes use money transfers to steal money from victims, buy fake goods, or obtain personal information. They can also take advantage of social media accounts by stealing them and using them for advertising or private gain.

5.4.4 Scams/Scammers

Participants 3 and 1 shared their experiences with scams:

> *P3: "Everything from 419 scams. which is basically when you receive an email that you won a million bucks or dollars. To access this money, you have to contact a certain person written in that email, and eventually, they will contact you back. They will then say if you want to access that money, you need to pay a certain amount or fee. They will extort more and more money from you, and eventually, when you figure out you have been coined, they will stop all communication with you"*

> *P1: "There is this thing called cryptocurrency where criminals will disguise themselves as maybe LUNO and convince you to buy crypto only to find that is actually a scammer and they are defrauding you."*

Ndubueze (2019) reports these types of crimes as Advance Fee Scams or fraud, where scammers target oblivious victims through emails. These emails are full of scams that seem to be from people who are giving away enormous sums of money to victims who just need to pay a little fee to have the money processed and sent to them.

Phishing and advance fee scams operate on the same fundamental principle.

5.4.5 Phishing Attacks

Phishing attacks were mentioned by participants 7, 8, and 16 as a common type of cybercrime in South Africa.

P7: "It is Phishing attacks that we see. You may get an email from a bank saying that someone is trying to access your account, you need to give them your details so that they can stop that activity. They will ask you to confirm your details so they can put a stop to it. Once they receive all those details, they will withdraw all your money"

P8: "Criminals are able to redirect or intercept emails to defraud people. I don't know how they do it, how do they know that if they send you a certain link you are going to click on it and they are then able to change even bank details that the money is supposed to go to, and its than transferred to them"

P16: "Phishing is very big, and it is very difficult to detect. Sometimes, criminals will send a link via email saying that you have to verify your information and change your PIN. Otherwise, your account will be closed or frozen. And it is always a matter of urgency. Once you click on that link or provide your details to that email, it's over. They will steal confidential information that they can use to defraud you"

Sawaneh (2020) states that phishing schemes are the most common type of online fraud in South Africa, and because they are so successful, they happen quite often. Phishing attacks involve cybercriminals posing as legitimate or well-known businesses in order to send you emails (Chudasama, Patel, Shah & Shaikh, 2020). Emails usually indicate or require an emergency response and may seem to be from trusted sources such as banks or e-commerce platforms (Joynt, 2023). Chudasama, Patel, Shah, and Shaikh, 2020; and shola, 2021 and Nnaemeka, (2023) further add that clicking on such links in your emails will direct you to a fraudulent website. Your sensitive information, such as your card number, UPI code, and other bank credentials, will be requested from you by the phony website. Additionally, going on these URLs can launch a computer virus on your system.

This theme revealed that all online crimes mentioned by participants seemed to fall under the category of Type 1 cybercrimes. Category 1 of cybercrimes involves utilizing computer-related and enabled technologies. They are mostly for financial gains and involve financial fraud, such as identity theft and online fraud.

Phishing, data theft, and manipulation via viruses or hacking are a few examples of Category I cybercrimes (Gumbi, 2018). South African cybercrimes seem to be different from the type II category of cybercrimes. Type II involves individuals, who can be considered more deceitful. They are interpersonal cybercrime, involving personal attacks and taunting of the reputation of a victim, such as cyberbullying, cyberstalking, child exploitation, extortion, and blackmail. Gumbi (2018) observes that it is not always easy to distinguish between the two categories of cybercrimes with precision; not all cybercrimes fall neatly into Type I or Type II categories. There are those that represent opposite ends of a continuum. According to the RAT, offenders spend a lot of time online to stay active and ensure maximum exposure to commit these crimes., for instance, hacking and fraud, mostly for financial gain (Holt' & Bossler, 2013).

5.5. Challenges that SAPS officers encounter in dealing with cybercrimes

Subsequently, in understanding and finding out the types of crimes that SAPS encounters, it was important to establish the root causes of the problem and the challenges surrounding cybercrimes. Knowing the problem and where it stems from allows the possibility of offering solutions.

5.5.1 The Causes of Cybercrimes

The majority of the views expressed by the participants on the causes of cybercrimes centered around the lack of knowledge of technology among South Africans. Both the public and law enforcement entities need to be more informed and knowledgeable in the advancement of technology and cybercrimes.

Participants 1, 3, and 5 expressed their views as follows:

P1: "In South Africa, I think it is the lack of knowledge in technology; the less you know about technology, the more you get scammed."

P3: "It is a Lack of knowledge by people that are using technology. People can deceive you that you won a lottery, and you know you have not played any lotto, but you still believe that you won all that money"

P5: "I think it is a lack of knowledge from the people. We are not that technically savvy. And Some people are so desperate that when they see something where they can get money easily, they do not ask or verify if something is legit."

These observations confirm Ismail's (2020) contention that lack of knowledge is one of the primary obstacles impeding the management of cybercrime and cyber security protocols.

There is a high potential for exploitation among internet users when they have little to no knowledge of the dangers of the technology they utilize. This further raises Africa's apprehensions about its potential to become a safe haven for cybercrimes. The lack of awareness regarding cyber- related hazards and risky behaviours could also influence how law enforcers investigate cybercrimes. Responding and/or investigating cybercrimes could prove to be challenging for police officers if they lack awareness.

Participants 2 and 12 further said:

P2: "Cybercrime is a new way of defrauding people, and the majority of police and investigators are not well informed and are not trained enough to investigate these crimes. "

P12: "I believe it is poor security, poor IT Security knowledge on the part of the individuals as well as the enterprises that conduct businesses. The internet is the main platform that they even conduct their day-to-day businesses, they must be knowledgeable in it"

Ndubueze (2020) states that the establishment of cybercrime laws in African nations can be hindered by a lack of knowledge regarding security risks associated with ICTs. The United Nations Commission for Africa has expressed dissatisfaction with stakeholders' lack of familiarity with these issues and has highlighted the necessity for increased ICT-related security knowledge for the effective creation and implementation of cybercrime laws, especially for professionals in the criminal justice system. Maluleke (2023) further asserts that a lack of knowledge and regulation around cyber security also draws attention to the fact that developing nations often lack even basic computer skills. Turianskyi (2018) also asserts that even lawmakers lack adequate knowledge of technology and the Internet, and this sometimes results in cybersecurity laws being poorly drafted and impractical.

The availability and accessibility of the internet and ICT devices is another factor mentioned by participants as a cause of cybercrime prevalence. Below are examples of responses from participants 6, 10, and 12:

P6: "I think it is because it is easy to do and there's no trace. The internet is more accessible and always accessible"

P10: "Online crimes are easy to do; you can do it anywhere, unlike contact crimes where you have to carry guns. Sometimes you can commit cybercrimes without even realizing it."

P14: "The causes are that it is not easily detected, and people sometimes use devices that cannot be traced, so it is very difficult to even trace the devices that they were using"

The quoted examples clearly confirm much of the literature; for instance, Baylon and Antwi-Boasiako (2017) maintain that while the growing internet infrastructure penetration poses challenges for law enforcement, it also makes it easier for cybercriminals to carry out their illicit activities. It enables them to swiftly and inexpensively defraud victims around the world. Because of this accessibility and availability, offenders are not only able to target victims in nearby places but can also target victims across borders. Cybersecurity experts are also concerned that broadband services are opening in the African continent, which means more users would be able to access the web as more people have easy access to these gadgets and can access or connect to the web, the more the chances of cyber offending. A major challenge is locating the cyber offenders for prosecution and conviction. Cyber offenders appear to be highly skilled, and it would require law enforcement officials of similar caliber and adequate resources to overcome and deal with them (Capazorio and Hollis, 2017).

Asked to comment on the causes of cybercrimes, some participants alluded to socio-economic pressures arising from, for example, poverty, unemployment, and negative personality traits such as greed and selfishness. Other participants also attributed it to a lack of awareness of the risks associated with Internet and online transactions.

Participants commented and stated

P15*: "Greed of people is also another factor; they never confirm anything they just want money*"

P17: *"It is because of social reasons, such as unemployment and poverty"*

P16: *"I think there is not enough media publicity on cybercrimes. We need more of that, yes banks do try to do that, but more can be done"*

The views of the participants resonate with much of the literature. Ismail (2020), for instance, says that many nations still struggle to develop national cyber security awareness programmes or campaigns. To eliminate or reduce cybercrime, public awareness, and education are critical. It is important to create educational initiatives to increase public awareness of cybercrime and how people can protect themselves (Van Vuuren, Leenen & Pieterse, 2020) . Gumbi (2018) advocates for cooperation between government, business, and civil society organizations in raising cyber security awareness to protect citizens, businesses, and state assets.

5.5.2 Challenges Experienced when Dealing with Cybercrimes

One of the aims of the study was to identify and understand the challenges Police Officers encounter in their day-to-day operations. Among the reported challenges were a lack of skills or inadequate capacity, time constraints, under-reporting, corruption and jurisdiction issues, and mutual agreements.

5.5.2.1 Lack of Skills and Inadequate Capacity

Asked about the challenges that they face, the majority of the sampled police officers indicated that most of their challenges were centered around lack of or inadequate capacity, particularly human resources, and equipment in the field of cyber security and online crimes. On human resources, the identified gaps were noticeable in terms of numbers, knowledge and skills. According to Nowacki and Willits (2019), the latter could be attributed to the fact that technological abilities are not given as much weight in the recruitment process as physical fitness and general knowledge.

A sample of the participant's responses is provided below:

P2: " Cybercrime is not new, but in South Africa or as SAPS, we are far behind in techniques used to investigate these crimes. Not many of us have much knowledge or expertise to investigate this crime. In a seminar I attended, it was reported that in South Africa, only about 100 people are qualified to investigate cybercrimes. In the whole police force. So how are we going to investigate so many cases that are coming in. we are also far behind in the knowledge that the criminals have. At the moment, we are falling behind and have a lot of catching up to do. Many police don't have the skills and the equipment to investigate."

P1: "Most of us do not have the forensic tools and licensed software's probes to conduct further investigations. It is frustrating when we can't achieve the goal of getting these offenders behind bars. We are lacking the tools and resources"

P12: "One challenge I encountered before was when I was assigned a case to one company that deals with IT, and when I went there, the first thing they asked me was what IT experience do I have? Although I have been investigating cybercrimes, I do get a lot of assistance from the IT specialist in our department who screens devices that we give them, and then, as forensic investigators, we assess links and analyse the data or information they have found. So, they were hesitant to work with me because they think I do not have the expertise they specifically need to handle the case."

P16: "Lack of knowledge on cybercrimes. I think extensive training is needed. We do not have training that can assist us in keeping up to date with these crimes. It is difficult to investigate cybercrime if you do not have the necessary knowledge."

P17: "Normally, most of our challenges are about skills; we need to develop skills or train our members. Although we have units, we are able to take computers and access and analyse that information. We still need more training. We need training that can allow us to be proactive rather than reactive to detect these crimes."

Evidently, education and training in Information Technology (IT) is a major issue that needs to be taken seriously. The backdrop of the evidence here is the UNDOC's (United Nations Office on Drugs and Crime) observation that barely half of committed law enforcement officials receive regular training, and 70% lack computer skills and equipment. This is certainly untenable given the seriousness of cybercrime in South Africa. Apparently, the judicial system and law enforcement authorities must continually invest in human resources as well as equipment, specifically computers, forensic tools, and licensed software, to improve the unit's capacity to curb cybercrime in South Africa (Świątkowska, 2020).

Świątkowska (2020) further states that Just 10,000 certified cybersecurity professionals work in Africa, despite the continent's 1.3 billion inhabitants.

Other participants commented:

P8: "We do not have a dedicated capacity. South Africa has nine provinces, with properly trained officers in the head office in Pretoria. Although they are trying to capacitate other provinces as we have an office as well, we are very limited, and most of us learn along the job."

P10: "It's getting challenging at times when so much is coming, and we only have like 5 people to investigate 20 dockets."

P14: "The challenge is logistics; we do not have enough members. Resources are a bit okay but sometimes we do not have internet. So how are we going to investigate cybercrimes if we do not have internet. The training needs to be upgraded. More training needs and more resources and manpower."

Van Vuuren, Leenen & Pieterse (2020) Support their opinions and submit that Cybercrime investigation units are short-staffed and lack adequate training. African nations are often challenged for their poor response to cybercrime because of insufficient resources for their law enforcement agencies' infrastructure, intelligence, and lack of employees. African nations seem

to primarily focus on addressing urgent problems like poverty alleviation and conventional offenses like stealing rape, and murder. The result is that the battle against cybercrime is not keeping up (Cordero & Thaw, 2020).

5.5.2.2 Time Constraints

Participant 9 mentions the investigating process of cybercrimes as very time-consuming:

P9 commented*: "Another challenge is the time period to investigate cybercrime; it is not quick. It takes time because if you look at an account where cybercrime was committed, the money was taken and transferred to different accounts. Everything must be analyzed, and once information has been analysed, then we can further use section 205. So, everything becomes time-consuming.*

If we have a team investigating a case it could be faster, but you find that I am investigating a certain case while I have all other cases that I have to investigate as well. Each complainant wants their case to be investigated first and the quickest, but unfortunately, this is not possible.

Time constraints are not only caused by laws and processes that they have to follow in their investigations but also by limited capacity in the police force, which is also an influence.

5.5.2.3 Corruption

Police officers are also concerned about corruption in their line of work. In South Africa, corruption-fueled cybercrime has resulted in insiders giving cyber criminals access to critical information, bypassing security systems and making it harder to detect (Richards & Eboibi, 2021).

Participants 7 and 13 stated regarding Corruption:

P7: "Sometimes challenges come from inside jobs, where you find that a criminal is either working with someone from inside the company, it can be at the bank or even within us."

P13: "Another problem we face is that these criminals work with the people from inside, or inside the banks, they do not follow procedures, and they quickly release the money to criminals so they can also benefit."

Richards and Eboibi (2021), for instance, argue that corruption is a result of poverty, greed, and the desire for wealth, and its appeal to perpetrators does not exclude insiders in the context of cybercrime on the continent. Cybercrime institutions and stakeholders, including law

enforcement agencies, financial institutions, and postal agencies, are not exempt from organized groups in Africa. In exchange for payment, bank employees and postal workers assist offenders in the clearance of items and money. Because corrupt law enforcement officials are more interested in taking bribes and abusing innocent individuals, some citizens are often reluctant to report cybercrimes. For example, con artists occasionally pay courts or police officers to ignore and disregard their actions or illegal acts (Baylon & Antwi-Boasiako, 2017). This discourages victims from reporting. As a result, law enforcement officials sometimes find some victims uncooperative, hindering their efforts in fighting against cybercrimes.

5.5.2.4 Underreporting

Although systems are in place for victims to report cybercrime, such as contact points or security hubs, the police officers reported underreporting as one of the challenges in South Africa.

The participants responded as follows:

P3: "One challenge is that cybercrime is not reported. Victims think that since I was scammed online, the police cannot find this, and if they go there, what will I say? And when they do report, some police stations do not know what they should do when they get these types of reports. For instance, if maybe you go to a police station in Zululand, sometimes they do not know the channels to follow."

P6: "People do not report these crimes. Sometimes, they don't report because you find that both of them were perpetrators or both individuals are involved. So, if I get scammed in the process, I cannot report it because I was also involved. It is more like corruption where we both get involved, and if I get cheated out of the deal, I cannot report it because I might implicate yourself"

Underreporting can be due to a variety of reasons, as mentioned by the participants and researchers. Victims may not report because they are also blamed for these offenses, and sometimes, they blame themselves for their carelessness and being victimized. Poor knowledge of cybercrime might also mean that many Internet users might become victims of cybercrime and not know if they should report it and how probable that they will receive assistance from law enforcement. Chudasama et al. (2020) argue that underreporting is caused by issues of trust in the police department. There seems to be a lack of confidence in victims in the police. Others do not report because they may view the offense as small and need not be reported as it had a low impact. In some cases, victims may also have no knowledge of how and where they

can report the crime (De Paoli et al., 2020 & Curtis & Oxburgh, 2022). When it comes to some businesses and organizations, they are often reluctant to disclose incidences of that nature to protect the company's or organization's image and reputation (De Paoli, Johnstone, Coull, Ferguson, Sinclair, Tomkins, Brown, & Martin,2020).

5.5.2.5 Jurisdiction Issues and Mutual Agreements

Cyber activities are an inherently cross-border phenomenon, with data transfer processes taking place in multiple countries and critical infrastructure being integrated into computer networks, making and exposing anyone as a target of cybercrime (Mabunda, 2021). Police officers are challenged by the borderless crime with any individual having easy access to the internet and an opportunity to victimize anyone anywhere in the world. This raises jurisdiction issues in international cybersecurity and safety matters.

According to Ndubueze (2020), jurisdiction refers to a country's right to regulate and punish offensive conduct. However, this right is often limited by physical boundaries and can only be exercised in accordance with international protocols, treaties, and conventions on cybersecurity and safety. This often poses a challenge to law enforcement agencies, and in this study some of the participants raised it.

Participants 5 and 11 commented as follows:

P5: "Jurisdiction issues are also what we encounter because you find that the scammer is not even here in South Africa when we follow the IP address. You find that maybe they are in America or England, and it becomes difficult to find and arrest that offender without going against other countries' laws. That also has financial implications for the government because if it happens that I do find that criminal then that means the government has to pay for that offender to be transported in South Africa to testify"

P11: "Some of the challenges I have encountered is that most of these perpetrators use Gmail and Gmail is not from South Africa. And to get access is a process which involves mutual legal agreements which is time-consuming."

Establishing jurisdiction in cyberspace is a major challenge in enforcing cybercrime legislation, especially for African countries dealing with cases that cut across multiple countries (Ndubueze, 2020). Physical proximity between the victim and the perpetrator is unnecessary for cybercrime. Participant 5 further addressed the issues of funding and resources needed to apprehend these criminals located in another country.

Gumbi (2018) supports the implications and states Because of jurisdictional challenges and the increased resources needed to track down cybercriminals across national borders, criminal laws governing cyberspace typically result in few prosecutions. Moreover, Reddy (2019) states that law enforcement's use of international standards for criminality causes extra expenses in terms of the amount of time and resources. Governments need to invest more and provide more funds to deal with cybercrimes. Without proper and enough funding, Criminal law enforcement mechanisms may not be able to provide sufficient deterrence to cybercrime (Orji, 2021). Jurisdiction issues also call for collaboration between organizations. Governments must establish efficient mechanisms for public-private cooperation through international initiatives Świątkowska, 2020).

5.6 Recommendations of intervention that SAPS adopt to curb cybercrime

Participants were asked what kind of technical support SAPS would need to make their work easier and more effective in combatting cybercrimes. They were also asked if they had any suggestions on how the public can protect themselves from cyber-offenders.

5.6.1 SAPS Perceptions on interventions to improve their capability to effectively decrease or respond to cybercrimes

The worldwide scope of cybercrime leads to uncertainty among and within law enforcement agencies, especially in African nations. Considering the shortcomings and difficulties that the participants had raised, opinions on possible solutions are necessary.

To effectively respond to cybercrimes, participants suggested:

P3: "We need more training and knowledge. they must train us more. We need more manpower and more resources to deal with cybercrimes. I think the programs that we use are very basic. we would overtly need more specialization to investigate cybercrime, and we always have to be one step ahead of the criminals; you have to understand exactly what is happening now."

P2: "Training people. Getting the necessary equipment to investigate and have programs to follow trends. These cost a lot of money, and sometimes, the government does not pay for all this. but We are far behind, and we need to be ahead like America or the developed countries because that is why now criminals are branching out and coming to us because we do not have the same standard to deal with these issues."

P4: "We need more training, and we will have more knowledge"

P6: "More training, training is the only way. Upgrades of equipment and more resources."

P8: "The focus must be on training police officers on cybercrimes. Expand units that specifically deal with cybercrimes. because although we do have them, we have a small number of police officers or members who deal with cybercrimes. We need more resources and computers that have specific software we can use to investigate these cases."

P11: "More training will help. We need forensic tools or investigative tools. We have to keep abreast of what is happening. it is not about once-off training because there are constant changes in technology every day, and the minds of criminals are changing every day. We can't use old techniques to investigate new or current crimes. Cybercrimes, unlike traditional crimes, change every day, so it's moving at a rapid speed.

The importance of human and financial resources and training in combatting cybercrime has been emphasized in the literature. Gumbi (2018), for instance, observes that specialized techniques and procedures are not always readily available or advanced enough to deal with the increasingly sophisticated cybercrimes that law enforcement officials encounter. The author further emphasizes that law enforcement officials should regularly and consistently be trained to investigate and prosecute cybercrime offenders. The training programs, according to Van Vuuren, Leenen, and Pieterse (2020), must focus on digital forensics strategies and the management of electronic evidence

Other participants noted the need to update training modules and encourage increased stakeholder cooperation.

Participant 12, for instance, drew attention to foreign exchange (forex) and cryptocurrency, saying,

"We need more training, especially on forex and bitcoin, because that is where crime is rife right now. Cybercriminals in South Africa mostly want money, so it is always financially related."

Indeed, police officers need to adapt to these new threats and enhance cybercrime detection, arrest, prosecution, and conviction.

Participants 10 and 15, on the other stated on collaboration with other stakeholders:

P10: "I think it is very important that we investigators get trained and work very closely with other private investigators from other organizations because these investigators know their systems as they change all the time. So, they can assist us in cases."

Collaboration is generally a favorably held proposition, particularly within security circles locally and internationally. More effective cybercrime measures at any level would require the involvement of various stakeholders, including prosecutors and the judiciary, private agencies/detectives or investigators, service providers, governments, and legislatures (Hjertstedt, 2019).

P15: "SAPS must work together with other international stakeholders. Because these people, when it comes to internet crimes, you find that it's international, not national. You find that a person who has committed the crimes is overseas, not this country. There must be good communication between stakeholders that deal with online crimes. And looking at the future, most of the crimes we are going to face in South Africa are online crimes. Because young people are now very sharp in technology, unlike before, so, this generation is different."

Cybercrime is a global issue; SAPS cannot work alone to control it.; governments at all levels must work together. Cross-border searches, seizures, extradition of cyber criminals, and the exchange of investigation leads should all be permitted under regional regulations (Ndubueze, 2020). A legal basis for international collaboration is provided by the Budapest Convention on Cybercrime, which regulates data preservation procedures and reciprocal legal aid.

The participants also recommended public awareness and workshops:

P6: "*I think the government must consistently do awareness campaigns and not wait for banks to be the ones that educate the public about cybercrimes. They can do that on radios, public walks, or some initiative to get the community involved. And they should broadcast and do awareness on radio stations such as Ukhozi or SABC, where even an average person also has access and can see this information.*"

P17: "In the past, we used to have workshops where all the detectives from different provinces come together, and we share information. It was based on a monthly or 3-month basis. But now it is so little, I think about once a year. So, different organizations will come, and banks will train us in the new trends. So, we need more of those workshops."

Indeed Van Vuuren, Leenen and Pieterse (2020) state that it is important to create educational initiatives to increase public knowledge of cybercrime concerns. Public websites, instructional materials, and resources tailored to certain industries and groups can all be used as a form of support. To promote safe online conduct, best practices for cybercrime should be created. This includes making low-cost tools for spotting online risks. Furthermore, South Africa should cooperate with businesses and society groups to raise cyber security knowledge.

An interesting suggestion was also brought forward by Participant 16:

"What we should do, FBI has done this before. They have recruited hackers to understand the minds of hackers and be in a position to have more arrests and convictions. so they must be recruited to work for law enforcement agencies, and we can use their skills to our advantage."

A study by Baylon and Antwi-Boasiako (2016) shared the same sentiments and stated that the fact that many online offenders can commit these complicated types of offenses shows that they do have technical skills. These skills could be utilized in the police force training schemes and information technology. Furthermore, development programs could be aimed at specifically providing youth with training to work for law enforcement or in various online roles within the public or private sector.

5.6.2 Perceptions on how the public can protect themselves from cybercrimes

The South African Banking Risk Information Centre (SABRIC) reports that the nation presently ranks third globally in terms of the number of victims of cybercrime, with an estimated R2.2 billion lost annually to cyberattacks (Gumbi, 2018). Law enforcement officers have to respond to the crimes and provide assistance to the victims. The study, therefore, asked the participant's views on how the public can stay safe and protect themselves from online crimes. It is important that the user of the internet and digital devices understands how to utilize these technologies while staying safe from cybercrimes.

All the participants acknowledged that it is important that users of the internet and digital devices understand how to utilize these technologies and stay safe from cybercriminals.
The responses of a few of them are provided below:

P1: "You must never give a person your private information, your account number, and ID numbers. And never give money to someone you do not know online."

P4: "Do not give out your pin numbers. These criminals even phone and pretend they are from a certain bank, and they ask for your PIN number because they want to change a debit order or some lie like that. And if you are gullible, you may give them your pin number, and then they will access all your accounts to scam you."

P5: "Don't allow or give a person, especially more a stranger, your personal information, such as passwords for your emails and your PIN, where they can have access to your bank Accounts."

Indeed, cybercriminals often use the victims' personal details to scam and defraud them. They either access the details directly from the victim, using deceptive strategies, hacking their accounts, or through emails (phishing links) to trick victims and steal their personal information. It is, therefore, important that individuals never give out their personal details to anyone to avoid being victimized by cybercriminals.

Other participants, specifically P10 and P14, advised the public on the use of passwords, pins, and firewalls; and investment in security software, as reflected in their comments below:

P10: "All devices should be locked; phones must have passwords, and laptops must have passwords, and it must be different passwords. If you use the same one where your PIN for the phone is the same as that of your bank PIN, I can be able to access those things."

P14: "Cybercriminals look at how you conduct your activities on the internet, and they identify your pattern, so constantly change your PIN and your security passwords. Do not use your names or passwords that have your date of birth or your children's names because then it would be easy to identify and unlock your password. They must also invest in security software like anti-virus software and talk to an IT specialist to assess security systems in their laptops and update them. Always update software because Windows always sends packages. Install firewalls when conducting business, and your privacy setting must be high."

Awoyemi, Omotayo, and Mpapalika (2021) explain that cybercriminals create malicious modems by evading security mechanisms using wireless routers like WPA2. A variety of passwords may be accessed unlawfully using such techniques. In this case, users must safeguard their accounts by regularly changing their passwords and adjusting their privacy settings on networking sites in accordance with cyber security procedures. Using anti-virus software, firewalls, and anti-phishing toolbars are further measures to guard against cyber assaults (Awoyemi, Omotayo & Mpapalika, 2021).

Participant 14 asserts that "*cybercriminals look at how you conduct your activities online and identify your pattern…"*

The Routine Activities Theory (RAT) supports the views in relation to cybercrimes that a suitable target may be associated with the types of activities an individual engages in while online (Navarro & Jasinski, 2015). The target's attractiveness may include the amount of time spent online, social network sites, use of online purchasing pages, banking, etc. When an individual connects to the internet, confidential information on the computer inadvertently transports valuable information into cyberspace, attracting offenders. Moreover, if the

motivated offenders possess sufficiently capable computer systems the target's inertia in cyberspace becomes almost weightless.

While some participants warned the public to be more careful and stay alert during festive seasons, others advised against phishing attacks.
Participant 8 commented as follows:

"These crimes always go up during the festive season. People are hungry, and they want money. That is also how they prey on their victims, making them promises only to scam them. Do not give out your pins. They must keep their identity or personal information very safe because these crimes are committed using people's stolen identities. Criminals can even use your address to deliver things. And then you find that your address will show that a certain purchase in a fraud case was delivered to your address"

Participants also advised against phishing attacks:

P2: "The best thing to do is verify if you get an email from ABSA, phone and verify with them. Do not use the numbers they gave you for verification. Search their phone number and ask if they sent an email to you and what it is about. If it looks suspicious, then don't ever respond. You always make enquiries"

P7: "If you get an email or link or messages that you do not know its source and are unsure where it comes from, delete it. If it comes from a legit source, they will call you and probably send you another email."

P3: "Avoiding opening links that you receive from people, avoid quick rich scams"
P11: "Simple advice, there's no money you can get without working for it, especially from a stranger. Because they expect something in return, and that is to scam you."

This study's findings confirm a study by Awoyemi, Omotayo, and Mpapalika (2021), which, among other things, advises the public to ignore links that show up in questionable or suspicious emails. Further to this crucial protective strategy, it is always prudent for one to limit one's online activity to secure websites, usually with `https' in their URL, or avoid opening links received from unknown sources. Doing so could save one from quick, rich scammers who promise victims enormous sums of money, using social engineering to trick them into paying a modest deposit in exchange for a larger sum of money. After paying the criminal, victims never hear from them again. Based on this reality, the police always warn the public against scammers: "If it seems too good to be true, then it probably is."

5.7 CONCLUSION

In this chapter, the findings of this study are presented and discussed. This study shows that the South African Police Services forensic units have systems in place to deal with cybercrimes in South Africa. Law enforcement officials employ various methods to fight against cybercrimes in the country. The methods include investigating various types of cybercrimes, including identity theft and online fraud, ransomware/cyber extortion, hacking, scams, and phishing attacks. They also engage in retrieving and analyzing digital data from computers and other digital devices, which, as digital evidence, they present in court to prosecute cybercrime offenders. This study also shows that while police interventions are somewhat effective, some challenges constrain law enforcement agencies' efforts. The challenges include lack of or inadequate capacity, particularly manpower complement, knowledge, and skills in ITC and equipment, specifically computers and software. Other challenges are corruption and jurisdiction, which pose challenges in enforcing cyber legislation in cross-border cybercrime cases. Although national and international measures or cyber instruments have been put in place to reduce or eliminate cybercrime, the phenomenon has been increasing. The increasing trend of cybercrimes and the dynamic modus operandi of cybercriminals complicate the already challenging law enforcement environment, making the work of digital forensic experts arguably more arduous. This implies that forensic units have to be adequately capacitated in terms of increased manpower and equipment to ensure adequate response to cybercrime in South Africa.

CHAPTER SIX
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter presents conclusions and a summary of the study. It discusses the summary or findings of the study based on the aim and objectives of the study. Recommendations are also made based on the study's findings, followed by concluding statements. This study explored how SAPS respond to cybercrimes and whether they have been effective in combatting cybercrimes or not, and the challenges, if any, they have been experiencing. This study also aimed to provide suggestions that could assist law enforcement agencies to be more effective in fighting against cybercrime in South Africa. The qualitative research method was adopted to collect and analyze data from a sample of 17 forensic experts drawn from the Forensic Unit of the South Africa Police Services in Durban.

6.2. Summary of the Key Findings

In summarizing the salient findings of this study, the following general conclusions were made considering the following objectives of the study:

- To identify the systems currently employed by SAPS to curb cybercrime.
- To determine the effectiveness of SAPS systems in responding to cybercrimes.
- To investigate the types of cybercrime that SAPS encounters
- To identify the challenges that SAPS encounters in dealing with cybercrime.
- To recommend interventions that SAPS can adopt to curb cybercrime

6.2.1 Systems Currently Employed by SAPS to Curb Cybercrime

This study found that the SAPS forensic unit is responsible for dealing with cybercrimes in South Africa. These officers possess the necessary knowledge and skills to investigate and convict cyber offenders. Their roles range from forensic investigators to investigative officers and Digital Forensic Investigators. Digital forensic investigators extract evidence from digital devices (Computers, phones, etc.). The way they respond to cybercrimes is office-based and concentrated on computers. These officers extract Digital traces left on digital devices or by every action taken on a person's computer system and a business network.

They trace IP addresses, messages, or anything from cookies and web browser history, even erased file fragments, emails, etc. Investigators or forensic investigators also play an essential role in responding to online crimes. The investigators go into the field to investigate cases. Before they begin with their investigations, they need to open a docket. The officers then need to gather evidence to prove that crime has occurred and prosecute offenders. The officer needs the right of authorization to gather evidence at a crime scene, such as consent or a court order. In accordance with Section 205, the Criminal Procedure Act 51 of 1977, police officers can subpoena (e.g., service providers, banks, offenders, etc.) and access confidential information that could be useful in cases.

They apply for a court order, and upon receiving permission from the court, the officers can quickly investigate the crime. The investigators may possess the victim's or offenders' devices or both and send the devices to digital forensic investigators to extract evidence from the devices (IP addresses, messages, etc). After extraction, the investigator needs to analyse and link evidence received from the digital investigator and build a case against the offender. Experts are necessary to investigate these types of crimes. Having an expert involved in a case ensured that no fabrication of evidence and data collected may be rendered as inadequate evidence in a court of law. This study further revealed that the nature of this crime requires collaboration to investigate or respond to cybercrimes. Police officers collaborate with Private companies such as commercial banks, security companies, and internet Providers (such as Vodacom, MTN, etc.) to decrease cybercrimes. As cybercrime is a global challenge, the importance of international collaboration was also emphasized. Cybercrimes committed outside South Africa are guarded by section 3 of the cybercrimes bill. Creating awareness of cybercrimes and working with SABRIC and banks was another way the police responded to cybercrimes. Indeed, this study revealed that SAPS, as a national law enforcement entity, is in line with the constitutional obligation to adopt and address the measures, policies, and strategies developed to deal with cybercrime. Investigators play a role not only in protecting the public and the country's economy, as most cybercrimes in South Africa appear to be mostly related to finances.

6.2.2 The Effectiveness of SAPS Systems in Responding to Cybercrimes

Evidently considerable efforts are being made by the police forensic unit to reduce or eliminate cybercrime and its impact in South Africa. To a considerable extent, some successes have been achieved. Although the successes were not quantified, participants did mention situations where they have achieved convictions, alluding to the belief that they could do better if they had more technical support from their political principals. This is in particular reference to manpower

(increased capacity) and advanced technical knowledge and skills in computer forensics; and equipment, such as computers and digital forensic software**.** This study further revealed that the units that deal with cybercrimes are still being developed in South Africa, and only a few currently exist to respond to cybercrimes. Therefore, although police officers make convictions and arrest online offenders, there are not many. They are still at a minimal percentage.

6.2.3 The Types of Cybercrime that SAPS Encounters

This study identified several online crimes that the officers encountered. The most prevalent were those classified as Type 1 cybercrimes. Type 1 cybercrimes involve financial fraud and the use of computer-related technologies. Cybercrimes in South Africa seem to be driven mainly by monetary gains, unlike Type II, which involves interpersonal cybercrimes like cyberstalking, child exploitation, extortion, and blackmail. Type II rarely occurs in South Africa but cannot be disregarded entirely as new ways of offending continue to shift in cyberspaces. Police officers mentioned hacking as a challenge. This crime requires offenders to hack into a system or computer to steal personal information, often leading to financial loss. They mentioned ransomware, where an offender may, for example, hack into a company's system and restrict access. They usually demand money to stop the attack or provide back access. Identity theft was also considered the most prevalent cybercrime. Offenders unlawfully access an individual's bank accounts or personal details and make unauthorized transactions or purchases. They may also steal and use an individual's social media accounts to advertise products. Victims may also be Scammed by being promised big sums of money. Lastly, police officers encounter phishing attacks. Phishing schemes were revealed to be the most common online fraud in South Africa. Cybercriminals pose as legitimate businesses and send emails with links requesting an emergency response. Clicking on these links leads to a fraudulent website, requesting sensitive information that they can use to defraud you and can potentially launch a computer virus on the user's system.

6.2.4 The Challenges that SAPS Encounters in Dealing with Cybercrimes

This study found that, indeed, there are some challenges constraining the efforts of law enforcement agencies combatting cybercrimes. The challenges include lack of or inadequate capacity, particularly financial and human resources; the latter relates specifically to inadequate manpower complement, digital forensic expertise (knowledge and technical skills in ITC) among the staff, and equipment, specifically computers and software.

The inadequacy of resources, apparently, does not only tend to cause delays in investigations, arrests, trials, and convictions; it also negatively impacts the efficiency and effectiveness of anti-cybercrime systems. It seems technological abilities are often overlooked in hiring digital policing, and police education and training are major challenges. South Africa is still trying to increase law enforcement authorities' capacity and capabilities. However, police organizations have found it difficult to adequately address the increased demands on their resources posed by the significant increase in cybercrime in recent years. Resources and expertise for preventing, identifying, and conducting cyberattack investigations are still limited. South Africa also struggles to develop effective cyber security awareness programs, successful campaigns, and educational programs essential to combat cybercrime.

There are issues related to corruption that have been challenging in South Africa for many years. This study found that even in the police force, it is a significant concern. Insiders in law enforcement, financial institutions, and postal agencies are part of organized groups that assist offenders in clearing items and money. Corruption hinders the efforts of ethical and law-abiding officers to decrease cybercrimes and help victims. Victims also do not report cybercrimes. Victims may not report due to blame, poor knowledge of cybercrime, or lack of confidence in the police department. At the same time, Businesses and organizations are reluctant to disclose victimization incidents to protect their brand values and shareholders' assets. Underreporting is a significant issue in South Africa and hinders effective cybercrime prevention and response strategies. This study also accounted for the fact that cybercrime is a cross-border phenomenon, and this presents challenges for police officers, as individuals have easy access to the internet and the opportunity to victimize anyone in any country. Jurisdiction, a country's right to regulate and punish conduct, is often limited by physical boundaries. Establishing jurisdiction in cyberspace is a major challenge in enforcing cybercrime legislation. Collaboration between organizations and efficient mechanisms for public-private cooperation through international initiatives is paramount.

6.2.5 Interventions that SAPS Can Adopt to Curb Cybercrime

This study revealed that regular digital forensic training and adequate resources are needed. Police officers need equipment such as computers with specific software used in investigating cybercrimes. Technology constantly changes, and a once-off training or course is not practical. Police officers must constantly keep updated on new technological developments, internet services, and emerging cybercrimes.

Moreover, stakeholders such as prosecutors, judiciary, private agencies, service providers, government, and parliament should be involved in tackling cybercrime. The global issue of cybercrime requires collaboration from national governments at all levels. There is a need for a proper and more close relationship between police officers and private companies to respond to cybercrimes effectively. Recruiting some offenders to work for the police force was also suggested. Online offenders possess advanced technical skills and can be utilized in police force training and information technology. This could provide job opportunities for offenders who commit these crimes for financial gain. Police officers are also advised to stay safe from online crimes; users must understand how to use digital devices and avoid giving out personal information. Cybercriminals often use victims' personal details to scam and defraud them. Users should regularly change passwords, adjust privacy settings on networking sites, and use anti-virus software, firewalls, and anti-phishing toolbars to guard against cyber assaults.

6.3 CONCLUSION

Law enforcement agencies are an important part of society, endowed with broad exclusive power to maintain law and order in all spheres of life and spatial domains, including cyberspace. With cybersecurity and safety becoming increasingly threatened as cybercrimes increase, the capacity of law enforcement agencies to maintain law and order, in this instance, in the sphere of cyberspace, comes under the spotlight. The findings, based on the perceptions and experiences of a sample of forensic police officers, indeed show that although the police have achieved some successes, their efforts are constrained by a number of challenges (such as lack of expertise and jurisdiction). Cybercrime is not only a national concern but also a worldwide concern, and at both levels, it may be understood from the perspectives of structural functionalist and rational activities theories. In that regard, combatting cybercrimes requires collaboration with stakeholders within and between countries. The data suggests that South Africa needs to invest continuously in cybersecurity to ensure online safety for the public and private sectors, as well as individuals. A strong information and communication technology system, a monitoring and evaluation system, stern enforcement of compliance with regulations and procedures, and prompt punitive action for non-compliance and against cybercriminals are all imperative in responding to cybercrimes effectively. Further, the government should use all available media channels to create awareness and decisively employ appropriate internal and external measures to support law enforcement agencies in dealing with cybercrime in South Africa.

6.4 RECOMMENDATIONS

It is evident in this study that the activities that jeopardize South Africa's cybersecurity and safety are on the rise while the enforcement of cyber instruments is lagging behind. Based on this observation, the following recommendations are made with the hope of strengthening the capacity of law enforcement agencies in combatting cybercrimes in South Africa:

6.4.1 Addressing Gaps in Security Systems and Innovations

Digital reality requires promoting innovative strategies to combat cybercrime. SAPS must develop and keep up to date with the latest security systems that provide a high degree of security for the country. Maintaining a national database that can assist in profiling cybercriminals and occasionally monitoring and evaluating the effectiveness of their strategies as part of the cybersecurity measures is very important. They must further develop systems that measure the extent of cyber enforcement challenges and the effectiveness of government efforts. The police or government can use AI, blockchain, and machine learning to reduce crime rates and protect the public. AI can quickly analyse vulnerabilities, identify frauds, scan emails, and prevent defects before attackers exploit them. This approach can help reduce crime rates and protect the public.

6.4.2 Awareness Campaigns and Reporting Systems

More awareness programmes and campaigns are needed. SAPS, working in collaboration with civil society organisations, needs to organize cyber-walks, seminars, workshops, and conferences to educate and train the public in not only the dangers of cybercrimes but also how they can protect themselves while using digital devices. The campaigns must focus, particularly, on rural and township communities where most residents are more likely to be less knowledgeable and skilled in using digital devices. Reporting systems must have cybersecurity task teams that operate 24 hours, can be easily accessed electronically, and can quickly respond to reports of online attacks. The government must also provide information on cybercrime risks to the public. This can go a long way in educating the public and helping prevent or combat cybercrimes in South Africa. For instance, such information could educate the public on where victims can report cybercrimes and provide a lead and/or intelligence on the extent and patterns of cybercrime, which could be invaluable to law enforcement agencies.

6.4.3 Advanced Training Methods

With the support of the government, SAPS must ensure that the way the cyber enforcement workforce is trained is modernised, adequately equipped, and skilled to deal with basic and sophisticated cybercrime issues. Training that fosters cybercrime evaluation and exercises is crucial for assessing the readiness of law enforcement in combatting cybercrimes. These exercises can be conducted quarterly through cybersecurity training workshops, with modules focusing on a combination of theoretical and practical online exercises, emphasizing the latter. The essence is to promote the development of advanced technical knowledge and digital forensic skills among the staff. The training must be consistently reviewed and updated from time to time to ensure that digital forensic officers are abreast with the dynamic cybersecurity environment.

6.4.4 Train the Youth

The youth are more technically savvy, and they are the ones who mostly engage in cyber offending. Development programmes that can train the youth are necessary. They can work in various online roles and capacities, e.g., with law enforcement agencies or campaign teams to educate the public and as facilitators at cyber education and training programs workshops. Training courses for ethical cyber security experts can be run at universities and colleges and should be encouraged. The government must also reinforce capacity-building programmes with the goal of targeting the people behind cyberattacks, especially given the increasing professionalisation of cybercrime, which involves business organisations as sponsors.

6.4.5 Research and Collaboration

SAPS must acquire a close partnership with academic institutions to encourage more research on cybercrimes. The SAPS research office should also focus on this.

6.4.6 Policies and Regulations

Cybercrime trends are constantly evolving, necessitating constant review of laws and strategies to address cybersecurity hazards. An institutional framework is needed to monitor information security systems and manage risks. Strong legal and administrative frameworks are also needed to combat cybercrime. In that regard, it is pertinent for the government to develop and enforce stricter laws, implying, for instance, heavier penalties for convicted cybercriminals. Further, periodic evaluations of laws and strategies are also necessary to keep abreast with the fast-changing cybercrime patterns and improve cybercrime policing in South Africa.

6.5 Recommendations for Future Research

More research is required to explore cybercrimes in South Africa. As can be noted, this study was limited to the KwaZulu Natal SAPS forensic unit; more research in other provinces could help authenticate the findings. A quantitative study or mixed methods for comparative purposes, and with a larger sample, could also be very helpful in substantiating the findings of this study for more conduct on the topic of cybercrime. The study could additionally explore cybercrimes through the lens of the public on how they understand cybercrimes and the risks of cybercrimes.

REFERENCES

Abdul-Rasheed, S.L, Lateef, I., Yinusa, M.A and Abdullateef, R.A (2016). Cybercrime and Nigeria's External Image: A Critical Assessment. Africology. *The Journal of Pan African Studies*, 9(6).

Akanle, O., Ademuson, A.O. and Shittu, O.S. (2020). Scope and Limitation of the Study in Social Research. Research. In Jegede, A.S. and Isiugo-Abanihe, U.C. (eds). Contemporary Issues in Social Research. Ibadan: Ibadan University Press. Pp. 105-114.

Alabi, A., Bamidele, A.H and Oladimeji, A.B. (2023). Cybercrime in Nigeria: Social Influence Affecting the Prevention and Control. *Lafia Journal of Economics and Management Sciences:* Volume 8, Issue 1; 2023.

Alansari, M. M., Aljazzaf, Z. M., and Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. In M. Sarfraz (Ed.), Developments in Information Security and Cybernetic Wars, pp. 1-41. IGI Global, Hershey, PA, USA. Available from: http://dx.doi.org/10.4018/978-1-5225-8304-2.ch001 (Accessed 30 March 2024).

Alase, A (2017). The Interpretative Phenomenological Analysis (IPA): A Guide to a Good Qualitative Research Approach. *International Journal of Education & Literacy Studies*, Vol. 5 (2).

Al-Dhaqm, A., Ikuesan, R.A., Kebande, V.R., Razak, S., Grispos, G., and Choo, K.R (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. Available from: https://doi.org/10.1109/ACCESS.2021.3124262 (Accessed 20 May 2024)

Alexandrou, A. (2021). Cybercrime and information technology: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices: CRC Press

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S. and Khan, M.K (2020). Comprehensive Review of Cybercrime Detection Techniques. Special Section on Emerging Approaches to Cyber Security, Vol 8. An Appraisal. *Dutse Journal of Criminology and Security Studies (DUJSCC),* 4(1), 78 – 88.

Andrade, C. (2021). The Inconvenient Truth About Convenience and Purposive Samples. Indian Journal of Psychological Medicine, Vol. 43, Issue 1.

Anney, V. N. (2014). 'Ensuring the quality of the findings of qualitative research: looking at trustworthiness criteria. *Journal of Emerging Trends in Educational Research and Policy Studies*, Vol. 5(2): 272–281.

Anwary, I (2022). The Role of Public Administration in Combating Cybercrime: An Analysis of the Legal Framework in Indonesia. *International Journal of Cyber Criminology*, Vol. 16(2): 216–227. Available from: https://orcid.org/0000-0002-4693-6467 (Accessed 11 July 2024)

Astalin, P.K. (2013). Qualitative Research Designs: A Conceptual Framework. *International*

Journal of Social Science & Interdisciplinary Research, Vol.2 (1).

Awoyemi, B. O., Omotayo, O.A. and Mpapalika, J.J. (2021). Globalization and Cyber Crimes: A Review of Forms and Effects of Cyber Crime in Nigeria. *International Journal of Multidisciplinary Research and Modern Education (IJMRME)*, Vol. 7(1), 2454 – 6119.

Babikian, J. (2023). Navigating Legal Frontiers: Exploring Emerging Issues in Cyber Law, Vol. 17, Issue No: 02. Available from: https://www.researchgate.net/publication/377964834 (Accessed 08 October 2024).

Bande, L.C. (2018). Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country Specific Specificities. *International Journal of Cyber Criminology*, Vol. 12 (1).

Bankole,F., Taiwo, A. and Claims, I. (2022). An extended digital forensic readiness and maturity model. Forensic Science International: Digital Investigation, Vol. 40

Bankole,F., Taiwo, A. and Claims, I. (2022). An extended digital forensic readiness and maturity model. *Forensic Science International: Digital Investigation*, Vol. 40.

Baror, S.O., Ikuesan, R.A. and Venter, H.S. (2021). A Defined Digital Forensic Criteria for Cybercrime Reporting. Available from: http://dx.doi.org/10.34190/ICCWS.20.056 (Accessed 11 March 2024).

Barrett, M. (2013). From stickups to mouse clicks: Cybercrime in Africa. Available From: https://www.defenceweb.co.za/joint/science-a-defence-technology/from-stickups-to-mouse-clicks-cybercrime-in-africa/ (Accessed 09 April 2021).

Bay, M. (2016). WHAT IS CYBERSECURITY? In search of an encompassing definition for the post-Snowden era. *French Journal for Media Research*, 6: 2264-4733.

Baylon, C, and Antwi-Boasiako, A. (2017). Chapter Six: Increasing Internet Connectivity While Combatting Cybercrime: Ghana as A Case Study. *Center for International Governance Innovation*. Available From: https://www.jstor.org/stable/resrep05239.11 (Accessed 2 June 2020).

Bekele, W. B. and Ago, F. Y. (2022). Sample Size for Interview in Qualitative Research in Social Sciences: A Guide to Novice Researchers. Research in Educational Policy and Management, Vol. 4(1), 42-50. Available at: https://doi.org/10.46303/repam.2022.3 (Accessed 07 August 2024).

Belli, L. (2021). Cybersecurity policymaking in the BRICS countries: From addressing national priorities to seeking international cooperation. *The African Journal of Information and Communication (AJIC)*, Vol. 28, 1-14. Available from: https://doi.org/10.23962/10539/32208 (Accessed 11 April 2024).

Bestoyin, K.O. (2018). Oil, Politics, and Conflicts in Sub-Saharan Africa: A Comparative Study of Nigeria and South Sudan. Historia Actual Online, Vol. 46 (2): 43-57.

Boda, R., Dullabh, R. and Steele, J. (2021). ENSafrica webinar: Cybercrimes Bill. Available from: https://www.ensafrica.com/videos/detail/3/ensafrica-webinar-how-the-cybercrimes-bill-wi (Accessed 17 June 2021).

Brown, C. S. D. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, Vol. 9 (1): 55–119.

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., and Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing*, Vol. 25(8) 652–661.

Capazorio, S and Hollis, R (2017). From Silk Road to Tor Tunnels: A Look at the History and Development of Cybercrimes. Cybercrime Law Feature. Available from: https://www.withoutprejudice.co.za/publication/2017/July/articles (Accessed 23 March 2019).

Cassim, F. (2011). Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. *The Comparative and International Law Journal of Southern Africa*, Vol. 44(1): 123-138.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, Vol 2 (1): 308–333.

Choi, K., Scott, T. M.; and LeClair, D. P. (2016). Ransomware against Police: Diagnosis of Risk Factors via Application of Cyber-Routine Activities Theory. *International Journal of Forensic Science & Pathology (IJFP)*, Vol. 4(7): 253-258. Available at: http://vc.bridgew.edu/crim_fac/29 (Accessed 15 Feb 2022).

Council of Europe (2001) Convention on Cybercrimes, European Treaties Series No. 185, https://www.coe.int/en/web/cybercrime/the-budapest-convention; https://rm.coe.int/1680081561 (Accessed: 12 December 2024.).

Chudasama, D., Patel, D., and Shaikh, N. (2020). Research on Cybercrime and its Policing. *American Journal of Computer Science and Engineering Survey*, Vol. 8 (3): 14. Available from: https://www.imedpub.com/computer-science-and-engineering-survey (Accessed 11 March 2024).

Cockcroft, T.W., Shan-A-Khuda, M. Schreuders, C. and Trevorrow, P. (2018). Police Cybercrime Training: Perceptions, Pedagogy and Policy. Policing: *A Journal of Policy and Practice.* Available from: https://doi.org/10.1093/police/pay078 (Accessed 21 June 2021).

Collier, B., Thomas, D.R., Clayton, R., Hutchings, A. and Chua, Y.T. (2022). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services, Policing and Society, Comparative Criminology, Vol. 65(4) 390– 408.

Cordero, C. and Thaw, D. (2020). Rebooting Congressional Cybersecurity Oversight. Vol. 32:1, 103-124. Available from: https://doi.org/10.1080/10439463.2021.1883608 (Accessed 08 October 2024).

Curtis, J. and Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal: Theory, Practice and Principles*. Vol. 96(4), 573– 592.

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G.,Tomkins, P., Brown, P and Martin, R. R. (2020) 'A qualitative exploratory study of the knowledge, forensic and legal challenges from the perspective of police cybercrime specialists. Policing (Oxford). Available From: https://doi.org/10.1093/police/paaa027 (Accessed 11 March 2024).

Degabasa, O. (2024). Cybercrime Threats and Trends in Ethiopia: Critical Legal Analysis. *Wallaga University Journal of Law*, Vol.1(2), 18-33. Available From: https://doi.org/10.20372/wujl.v1i2.1074 (Accessed 13 May 2024).

Demerath, N.J. (1966). Synecdoche and Structural-Functionalism. Social Forces. Vol. 44 (3): 390-401. Available from: https://www.jstor.org/stable/2575840 (Accessed 06 0ctober 2021).

Deora, R.S. and Chudasama, D. (2021). Brief Study of Cybercrime on an Internet. *Journal of Communication Engineering & Systems*, Vol. 11(1). Available from: http://computerjournals.stmjournals.in/index.php/JoCES/index (Accessed 11 March 2024).

Dlamini, S. and Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges, and effective responses, Cogent Social Sciences, Vol. 5 (1), Available From: https://doi.org/10.1080/23311886.2019.1675404 (Accessed 20 May 2024).

Du Toit, R., Hadebe, P.N and Mphatheni, M. (2018). Public Perceptions of Cybersecurity: A South African Context. *Acta Criminologica: Southern African Journal of Criminology*, 31(3).

Enweonwu, O.A., Ugwu, I.P., Onyejegbu, D.C, Areh, C.E and Ajah, B.O (2021). Religious Fanaticism and Changing Patterns of Violent Crime in Nigeria. *International Journal of Criminology and Sociology*, 10:1378-1389.

Eoyang, M., Peters, A., Mehta, I and Gaskew, B. (2018). To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors. Available from: http://www.jstor.com/stable/resrep20153 (Accessed 17 June 2021).

Etikan, I., Musa, S.A. and Alkassim, R.S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, Vol. 5(1): 1-4. Available At: http://www.sciencepublishinggroup.com/j/ajtas (Accessed 07 August 2024).

Errasti-Ibarrondo, B., Jordan, J.A., Dıez-Del-Corral, M.P., and Arantzamendi, M. (2018), Conducting phenomenological research: Rationalizing the methods and rigour of the phenomenology of practice. *Journal of Advanced Nursing*, Vol. 74 (7):1723-1734.

Garg, R. (2016). Methodology for research. Indian Journal of Anaesthesia. Vol. 60, Issue 9.

Gishuru, M.J. (2017). The Interpretive Research Paradigm: A Critical Review Of Is Research Methodologies. *International Journal of Innovative Research and Advanced Studies* (IJIRAS), Vol. 4, Issue 2.

Gojali, D.S. (2023). Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective. *International Journal of Cyber Criminology*, Vol. 1 7 (1): 1- 11.

Goundar, S. (2012). Research Methodology and Research Method: Methods Commonly Used by Researchers. Victoria University of Wellington.

Govender, T.F (2018). A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa. College of Law and Management Studies, University of KwaZulu-Natal.

Gumbi, D. (2018). 'Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States, and the United Kingdom.

Hassan and Khairuldin, (2020). Research Design Based on Fatwa Making Process: An Exploratory Study. *International Journal of Higher Education*, Vol. 9 (6). Available at: http://ijhe.sciedupress.com (Accessed 12 August 2024).

Hjertstedt, E.B. (2019). Cybercrimes Using Electronical Identification: What are the Dangers for Criminality? Health and Society, Malmo University.

Hofmeyr, C.D. (2020). The Cybercrimes Bill is one step away from becoming law. Technology, Media & Telecommunications Alert. Available from: file:///C:/Users/Slindile/OneDrive/Documents/articles/Technology-Media-Telecommunications-ALert-7-July-2020%20(1).pdf (Accessed 4 May 2024).

Holt', T.J and Bossler, A. M (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. journal of Contemporary Criminal Justice, Vol. 29(4): 420-436.

Holt, T.J., Turner, N.D, Freilich, J.D and Chermak, S.M (2021). Examining the Characteristics That Differentiate Jihadi Associated Cyberattacks Using Routine Activities Theory. Social Science Computer Review, 1-17. DOI: 10.1177/08944393211023324

Hosani, H.A., Yousef, M., Al Shouq, S., Iqbal, F. and Mouheb, D. (2019). A Comparative Analysis of Cyberbullying and Cyberstalking Laws in the UAE, US, UK, AND CANADA. Available From: https://doi.org/10.1109/AICCSA47632.2019.9035368 (Accessed 20 May 2024).

ITU (2021) (International Telecommunication Union) (2021). Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. Available from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (Accessed 12 November 2024).

Idowu, O.A. (2021). Cybercrimes and Challenges of Cyber-Security in Nigeria. *International Journal of Sociology and Development*, Vol. 3 (1).

Ismail, U. (2020). The Nigeria Police Force and Cybercrime Policing: An Appraisal. *Dutse Journal of Criminology and Security Studies (DUJSCC)*, 4(1), 78 – 88.

Johnson, D., Faulkner, E., Meredith, G. and Wilson, T.J. (2020). Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts. *The Journal of Criminal Law*, Vol. 84(5), 427–450.

Joynt, H.I. (2023). The South African legal framework's response to the prevalence of cybercrime in electronic commerce. Trade and Business Law, North-West University.

Kagita, M.K., Thilakarathne, N., Gadekallu, T.R., Maddikunta, P.K.R. and Singh, S. (2020).

A Review on Cyber Crimes on the Internet of Things. Available from: http://dx.doi.org/10.1007/978-981-16-6186-0_4. (Accessed 11 March 2024).

Kalu, F. A., and Bwalya, J. C. (2017). What Makes Qualitative Research Good Research? An Exploratory Analysis of Critical Elements. *International Journal of Social Science Research*, 5(2), 43-56. Available from: https://doi.org/10.5296/ijssr.v5i2.10711

(Accessed 05 August 2024).

Kang, E. and Hwang, H. (2023). The Importance of Anonymity and Confidentiality for Conducting Survey Research. *Journal of Research and Publication Ethics*, Vol 4 (1):1-7. Available from: http://dx.doi.org/10.15722/jrpe.4.1.202303.1 (Accessed 14 August 2024).

Kazaure, A.A., Jantan, A. & Yusoff, M.N. (2023). Digital Forensics Investigation Approaches in Mitigating Cybercrimes: A Review. *Journal of Information Science Theory and Practice*, Vol. 11(4): 14-39. Available from: https://doi.org/10.1633/JISTaP.2023.11.4.2 (Accessed 4 May 2023).

Kempen, A. (2019). Fighting cybercrime requires an integrated and international effort - The SAPS's envisaged approach. Servamus Community-Based Safety and Security Magazine. Available From: https://hdl.handle.net/10520/EJC-130abd8806 (Accessed 23 March 2021).

Khan, S., Saleh,T., Dorasamy, M., Khan,N., Leng, O.T.S., and Vergara, R.G. (2023). A systematic literature review on cybercrime legislation. Faculty of Management, Multimedia University.

Kılınç, H., and Fırat, M. (2017). Opinions of expert academicians on online data collection and voluntary participation in social sciences research. Educational Sciences: Theory & Practice, Vol.17, 1461–1486. Available from: http://dx.doi.org/10.12738/estp.2017.5.0261

Koziarski, J. and Lee, J.R. (2019). Connecting evidence-based policing and cybercrime. Policing and cybercrime. Available From: https://www.emerald.com/insight/1363-951X.htm (Accessed 21 June 2021).

Kritzinger, E. and Von Solms, S.H. (2012). A Framework for Cyber Security in Africa. *Journal of Information Assurance & Cybersecurity*. Available from: http://www.ibimapublishing.com/journals/JIACS/jiacs.html (Accessed 11 May 2021).

Kshetri, N (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2): 77-81.

Kuzior, A., Tiutiunyk, I., Zielińska, A., and Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2), 220-239.

Li, X. (2018). Crucial Elements in Law Enforcement against Cybercrime. *International Journal of Information Security Science,* (7)3.

Lourie, G. (2015). What is South Africa doing to Reduce Cybercrime—Tech Financials, Available From:https://www.techfinancials.co.za/2015/11/05/what-sa-is-doing-to-reduce-cybercrime/ (Accessed 23 March 2021).

Mabaso, J. (2018). Assessing the Cyber-Security Status of the Metropolitan Municipalities in South Africa. College of Law & Management Studies, University of KwaZulu Natal.

Mabunda, S.M. (2021). The South African Legislative Response to Cybercrime. Department of Criminal Justice and Procedure, Faculty of Law. University of Western Cape.

Maimon,D. Kamerdze, A. Cukier, M and Sobesto, B. (2013). Daily Trends and Origin of Computer-Focused Crimes Against a Large University Computer Network: An Application of the Routine-Activities and Lifestyle Perspective. The British Journal of Criminology, Vol. 53 (2): 319-343. Available from: https://www.jstor.org/stable/23640017 (Accessed 20 July 2021).

Maldonado, R. R. (2008). A Phenomenological Pilot Study of Energy Healers Expertise and Recommendations for Energetic Disaster and Trauma Relief Training. Akamai University.

Maluleke, W. (2023). Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa. *International Journal of Social Science Research and Review*. Vol. 6 (6), 223-243. Available from: http://dx.doi.org/10.47814/ijssrr.v6i6.1360 (Accessed 11 March 2024).

Mandal, J. and Parija, S. C. (2014). Informed Consent and Research. Department of Microbiology, JIPMER, Puducherry, India, Vol. 4, Issue 2.

Mapimele, F. and Mangoale, B. (2019). The Cybercrime Combating Platform Council of Scientific and Industrial Research (CSIR), Defence, Peace, Safety, and Security, Pretoria, South Africa.

Mason, M. (2010). Sample Size and Saturation in PhD Studies. Forum: Qualitative

Masthead (2020). Cybercrime in South Africa. Available at: https://www.masthead.co.za/newsletter/cybercrime-in-south-africa/ (Accessed 08 August 2024).

Matthew, O.F. (2016). Sociological and technological factors that enhance cybercrime and cyber security in Nigeria. *International Journal of Law and Legal Studies*, Vol. 4 (5): 207-216. Available from: https://www.internationalscholarsjournals.org/print.php?article=sociological-and-tech (Accessed 05 October 2021).

Miller, J. (2013) Individual Offending, Routine Activities, and Activity Settings: OGE Revisiting the Routine Activity Theory of General Deviance. *Journal of Research in Crime and Delinquency*, 50(3) 390-416.

Miller, C.M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. Forensic Science International: Synergy, Vol. 6.

Morrow, P.C. (1978). Functionalism, Conflict Theory and the Synthesis Syndrome in Sociology. *International Review of Modern Sociology*, Vol. 8 (2): 209-225. Available from: https://www.jstor.org/stable/41420656 (Accessed 06 October 2021).

Mtuze, S.S. and Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, Vol. 4, 299–323. Available from: https://doi.org/10.1365/s43439-023-00089-8 (Accessed 20 May 2024).

Mtuze, S.S. (2022). The convergence of legislation on cybercrime and data protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013. School of Law, Nelson Mandela University.

Mugisha, D. (2019). Role and Impact of Digital Forensics in Cyber Crime Investigations. *International Journal of Cyber Criminology*. Forensic Science Institute, Gujarat Forensic Sciences University (GFSU).

Muller, L.P. (2015). Cyber Security Capacity Building in Developing Countries. Norwegian Institute for International Affairs. Available From: https://www.jstor.org/stable/resrep07959 (Accessed 02 June 2020).

Muller, L.P. (2015). Cyber Security Capacity Building in Developing Countries.

Norwegian Institute for International Affairs. Available From: https://www.jstor.org/stable/resrep07959 (Accessed 02 June 2020).

Naeem, M., Ozuem, W., Howell, K. and Ranfagni, S. (2023). A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. International Journal of Qualitative Methods, Vol. 22: 1–18.

Navarro, J.N and Jasinski, J.L. (2015). Demographic and Motivation Differences Among Online Sex Offenders by Type of Offense: An Exploration of Routine Activities Theories. Journal of Child Sexual Abuse, 24:753-771.

Ndubueze, P.N. (2020). Cybercrime and Legislation in an African Context. Available from: http://dx.doi.org/10.1007/978-3-319-78440-3_74 (Accessed 11 March 2024).

Nduka, R.E. & Basdeo, V. (2022). The Need for Harmonised and Specialised Global Legislation to Address the Growing Spectre of Cybercrime. Southern African Public Law. Available from: https://doi.org/10.25159/2522-6800/8112 (Accessed 11 March 2024).

Negrin, K.A., Slaughter, S.E., Dahlke, S. and Olson, J. (2022). Successful Recruitment to Qualitative Research: A Critical Reflection. *International Journal of Qualitative Methods*, Vol. 21: 1–12.

Nijhawan,L.P., Janodia, M.D., Muddukrishna, B.S., Bhat, K.M., Bairy, K.L., Udupa, N and Musmade, P.B. (2013). Informed consent: Issues and challenges. *Journal of Advanced Pharmaceutical Technology & Research*, Vol. 4, Issue 3. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3777303/ (Accessed 03 August 2024).

Nkosi, L (2018). An Exploratory Study on Responses of South African Police Service and Non-Governmental Organisations to Human Trafficking in Durban Policing Area. School of Applied Human Sciences, University of KwaZulu-Natal.

Nnaemeka, E. (2023). Cybercrime and Online Safety: Addressing the challenges and solutions related to cybercrime, online fraud, and ensuring a safe digital environment for all users— A Case of African States. *International Research Journal*, Vol. 10 (9).

Nowacki, J. and Willits, D. (2019). An organizational approach to understanding police response to cybercrime. Policing: *An International Journal*, Vol. 43 (1), 63-76.

Nowell, L.S., Norris, J. M., White, D. E and Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, Vol.16: 1-13. SAGE publications.

Ogunlana, S.O. (2019). Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies. *Journal of Strategic Security* Vol. 12(1):72-106. Available from: https://scholarcommons.usf.edu/jss/vol12/iss1/4 (Accessed 20 July 2021).

Olayemi, O.J (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, 6(3): 116-125.

Olofinbiyi, S.A. (2022). A Reassessment of Public Awareness and Legislative Framework on Cybersecurity in South Africa. ScienceRise: *Juridicial Science*, Vol. 2 (20), 34–42. Available From: http://doi.org/10.15587/2523-4153.2022.259764

(Accessed 11 March 2024)

Orji, U.J. (2021). Moving Beyond Criminal Law Responses to Cybersecurity Governance in Africa. *International Journal of Criminal Justice*, Vol. 3(1), 60-98. Available from: http://dx.doi.org/10.36889/IJCJ.2021.002 (Accessed 13 May 2024).

Pandey, A.K., Tripathi, A.K., Kapil, G., Singh, V. Khan, M.W. Agrawal, A., Kumar, R. and Khan, R.A. (2020) Current Challenges of Digital Forensics in Cyber Security Chapter 3. Available from: https://doi.org/10.4018/978-1-7998-1558-7.ch003 (Accessed 14 May 2024).

Pasaribu, R. (2018). Fight Narcotics with Community Strengthening: Crime Control Management by Community Policing. *Journal of Indonesian Legal Studies*, Vol 3(2): 237-252.

Pathak, V.C (2017). Phenomenological Research: A Study of Lived Experiences Vinay Chandra Pathak. *International Journal of Advance Research and Innovative Ideas in Education* (*IJARIIE)*, Vol-3 Issue-1.

Ralarala, S. (2020). The impact of cybercrime on e-commerce and regulation in Kenya, South Africa, and the United Kingdom. School of Law, Strathmore University.

Reddy, E. (2019). Analysing the Investigation and Prosecution of Cryptocurrency Crime as Provided for by the South African Cybercrimes Bill. *Statute Law Review*, Vol. 20 (20), 1–14.

Reyns, B.W., Henson, B. and Fisher, B.S. (2011). Being Pursued Online: Applying Cyberlife Style-Routine Activities Theory to Cyberstalking Victimization. Criminal Justice and Behavior, Vol. 38(11): 1149-1169.

Richards, N.U. and Eboibi, F.E., (2021). African Governments and the Influence of Corruption on the Proliferation of Cybercrime in Africa: Wherein Lies the Rule of Law? *International Review of Law, Computers & Technology*, Vol. 35 (2), 131-161.

Rustad, M.L. (2001). Private Enforcement of Cybercrime on the Electronic Frontier. *Southern California Interdisciplinary Law Journal*, Vol. 11:63.

Ruslin, Mashuri S., Rasak, M.S.A, Alhabsyi, F. and Syam, H. (2022). Semi-structured Interview: A Methodological Reflection on the Development of a Qualitative Research Instrument in Educational Studies. *Journal of Research & Method in Education*, Volume 12, Issue 1, 22-29.

Sammons, J. and Cross, M. (2017). The Basics of Cyber Safety. Safety and Mobile Device Made Easy.

Sawaneh, I. A. (2020). Cybercrimes: Threats, Challenges, Awareness, and Solutions in Sierra Leone. *Asian Journal Interdisciplinary Research*, Vol. 3 (1). Available From: https://doi.org/10.34256/ajir20114 (Accessed 11 March 2024).

Slotta, D. (2023). Growth rate of cybercrime cases in China 2017-2020. Available from: https://www.statista.com/statistics/1422840/china-growth-rate-of-cybercrime-cases/ (Accessed 05 March 2024).

Shola, A.T. (2021). Poverty, Cybercrime and National Security in Nigeria. *Journal of Contemporary Sociological Issues,* Vol. 1:2, pp. 86-109.

Smith, J. and Firth, J. (2011). Qualitative data analysis: application of the framework approach. Nurse Researcher, Vol.18 (2): 52-62.

Sovacool, B.K., Iskandarova, M. and Hall, J. (2023). Industrializing theories: A thematic analysis of conceptual frameworks and typologies for industrial sociotechnical change in a low-carbon future. Energy Research & Social Science, Vol. 97.

Srinivas, T.A. S, Donald, A. D, Thippanna, G., Madiletty, C and Thanmai, B.T. 2023). Exploring the Uncharted: A Research Problem Statement. Recent Trends in Androids and IOS Applications, Vol. 5, Issue 3. Available from: https://doi.org/10.5281/zenodo.8214100 (Accessed 08 October 2024).

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. The European Cybersecurity Forum -CYBERSEC *and* AGH University of Science and Technology.

Stats SA (2024). Improving lives through Data Ecosystems. Available from: https://www.statssa.gov.za/?p=17440 (Accessed 28 March 2025).

Tomkins, K (2005). Police, Law Enforcement and the Environment, Current Issues in Criminal Justice, Vol. 16:3, 294-306. Available From: https://doi.org/10.1080/10345329.2005.12036326 (Accessed 08 October 2024).

Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. computer law & security review Vol. 34, 1197–1214. Available from:https://www.researchgate.net/publication/327501929_Rethinking_Privacy_in_the_Co uncil_of_Europe's_Convention_on_Cybercrime (Accessed 16 July 2024).

Turianskyi, Y. (2018). Balancing Cyber Security and Internet Freedom in Africa. South African Institute of International Affairs. Available from: https://www.jstor.org/stable/resrep25912 (Accessed 17 June 2021).

Turianskyi, Y. (2020). Cyber Governance Lessons. South African Institute of International Affairs. Available from: https://www.jstor.org/stable/resrep25957 (Accessed 17 June 2021).

Van Vuuren, J.C, Leenen, L. and Pieterse, P. (2020). Development and Implementation of Cybercrime Strategies in Africa with Specific Reference to South Africa. *Journal of Information Warfare*, Vol. 19 (3), pp. 83-101. Available from: https://www.jstor.org/stable/10.2307/27033634 (Accessed 11 March 2024).

Verizon Business (2023). 2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket. Available from: https://www.verizon.com/about/news/2023-data-breach-investigations-report (Accessed 16 November 2024).

Wang, S.K., Hsieh, M., Chang, C.K., Jiang, P. and Dallier, D.J. (2020). Collaboration between Law Enforcement Agencies in Combating Cybercrime: Implications of a Taiwanese Case Study about ATM Hacking. *International Journal of Offender Therapy and Comparative Criminology*, Vol. 65, Issue 4.

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. The British Journal of Criminology, 56, Issue 1, 21–48. Available from: https://doi.org/10.1093/bjc/azv011 (Accessed 15 Feb 2022).

Williams, M.L, Levi, M., Burnap, P. and Gundur, R.V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. Deviant Behavior, Vol. 40(9):1119–1131.

Wu, T., Breitinger, F and O'Shaughnessy, S. (2020). Digital forensic tools: Recent advances and enhancing the status quo. Forensic Science International: Digital Investigation, Vol. 34. Available from: https://doi.org/10.1016/j.fsidi.2020.300999 (Accessed 24 July 2024).

Yar, M. (2005). The novelty of 'Cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, Vol. *2*(4): 407–427.

Younes, M.A.B. (2019). Internet Fraud to Deceive Email by Using Different Technologies. International Journal of Advanced Research in Computer Science, Vol. 10 (1). Available

from: http://dx.doi.org/10.26483/ijarcs.v10i1.6349 (Accessed 21 June 2021).

APPENDIX i: Participants Informed Consent Form

UKZN HUMANITIES AND SOCIAL SCIENCES RESEARCH ETHICS

COMMITTEE (HSSREC)

APPLICATION FOR ETHICS APPROVAL
For research with human participants

INFORMED CONSENT RESOURCE TEMPLATE

Note to researchers: Notwithstanding the need for scientific and legal accuracy, every effort should be made to produce a consent document that is as linguistically clear and simple as possible without omitting important details, as outlined below. Certified translated versions will be required once the original version is approved.

There are specific circumstances where witnessed verbal consent might be acceptable, and circumstances where individual informed consent may be waived by HSSREC.

Information Sheet and Consent to Participate in Research

An Exploratory Study of the South African Police Services Systems in Combating Cybercrimes.

Date:

Dear sir/madam

You are hereby being invited to participate in a research study. The study will be conducted by Slindile Ngcece a PhD student from the Criminology and Forensic department at Howard College. Participation is voluntary. Please take as much time as you need to read the consent form. For any enquiries that you may have feel free to contact me at [redacted] or email me at 214519385@stu.ukzn.ac.za.

Purpose of the study
You are invited to consider participating in a study involving research to answer a few questions about cybercrimes. The aim and purpose of this research are to find out how SAPS deals with or combat cybercrimes. It is to explore the systems SAPS uses to combat cybercrimes and their effectiveness. The researcher would like to know your views on cybercrime, the kinds of cybercrimes, and the challenges that SAPS encounters when dealing with cybercrimes. Lastly, the researcher would like to know your views on what needs to be done or improved that could assist the police officials in doing their jobs efficiently.

Procedures
The study is expected to interview participants, from the SAPS Commercial Crimes Unit and the Directorate of Priority of Crimes Unit. The law enforcement officials will be interviewed individually in their respective posts (or preferred locations) and in their willingness to be part of the study. The police officials will be asked some questions regarding cybercrimes in South Africa. The duration of your participation, if you choose to enroll and remain in the study, is expected to take not more than 30 minutes.

Risks and/or discomfort

There is no anticipated risk for participation in this study. However, when you feel discomfort answering some of the questions, you may ask to skip the question, take a break, or withdraw from participation.

This study has been ethically reviewed and approved by the UKZN Humanities and Social Sciences Research Ethics Committee (approval number____).

In the event of any problems or concerns/questions, you may contact the researcher at [redacted] or email at 214519385@stu.ukzn.ac.za. or the UKZN Humanities & Social Sciences Research Ethics Committee, contact details as follows:

HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION
Research Office, Westville Campus
Govan Mbeki Building
Private Bag X 54001
Durban
4000
KwaZulu-Natal, SOUTH AFRICA
Tel: 27 31 2604557- Fax: 27 31 2604609
Email: HSSREC@ukzn.ac.za

Participation and withdrawal
Participation in this study is voluntary. If you volunteer to be part of the study, you may choose to withdraw anytime. You may also choose not to answer a question when you feel uncomfortable and remain in the study. The researcher may pull you out of the study when circumstances arise which require doing so. Other alternatives are not to participate.

Penalty and/or rights of participants
You may withdraw your consent to participate at any time. There are no penalties for withdrawing from the study. You may continue or discontinue without any legal claims for participation in the study. No cost will be incurred for participation. There are no financial or reimbursements for participation in the study.

Confidentiality
Confidentiality will be ensured for participants. Any information obtained from the study that can relate to you will be kept confidential and may only be disclosed with your permission or when required by law. Pseudonyms will be used to ensure that your identity is not revealed at any stage. The real names of participants, their places of residence, and all responses will be kept separately from the rest of the data. The researcher will use an audiotape to record all the information with prior consent from the participants. The recordings will be kept secure and confidential in case there is a need for future reference. Upon completion of the research write-up, all tapes will be destroyed. The researcher will transcribe the recordings and may provide you with the transcript if requested. Responses that you may ask to leave out will not be used and will be removed from the data. Upon publications discussions, or conferences, no information will be included that will reveal your identity. All the information obtained will be used for academic purposes only.

CONSENT

I..... have been informed about the study entitled "An exploratory study of the South African Police Services systems in combating cybercrime" by Slindile Ngcece

I understand the purpose and procedures of the study (add these again if appropriate).

I have been allowed to answer questions about the study and have had answers to my satisfaction.

I declare that my participation in this study is entirely voluntary and that I may withdraw at any time without affecting any of the benefits I am usually entitled to.

I have been informed about any available compensation or medical treatment if injury occurs to me because of study-related procedures.

If I have any further questions/concerns or queries related to the study, I understand that I may contact the researcher at (email 214519385@stu.ukzn.ac.za).

If I have any questions or concerns about my rights as a study participant, or if I am concerned about an aspect of the study or the researchers, then I may contact:

HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION
Research Office, Westville Campus
Govan Mbeki Building
Private Bag X 54001 Durban
4000
KwaZulu-Natal, SOUTH AFRICA
Tel: 27 31 2604557 - Fax: 27 31 2604609
Email: HSSREC@ukzn.ac.za

Additional consent, where applicable

I hereby provide consent to: Audio-record my interview YES / NO

Signature of Participant	**Date**
Signature of Witness (Where applicable)	**Date**
Signature of Translator (Where applicable)	**Date**

APPENDIX ii: Interview Schedule

An exploratory study of the South African police services (SAPS) systems in combating cybercrime.

Interview Questions:

1. What is your role in this division?
2. What are your thoughts about cybercrimes in South Africa?
3. What types of cybercrimes do you usually encounter in your organization?
4. What do you think causes cybercrimes or these types of crimes in South Africa?
5. What are some of the procedures do you use to deal with or respond to cybercrimes?
6. To what extent has the SAPS been successful or able to decrease and convict cybercriminals?
7. What are some of the challenges you encounter (if any) when dealing with these crimes?
8. How has working in this division or dealing with these crimes affected your overall job satisfaction?
9. How would you advise the South African public to stay safe from cybercrimes?
10. What are some of the things you think should be done or improved for SAPS to decrease cybercrimes effectively?

APPENDIX iii: School of Applied Human Sciences Approval Letter

Dear Slindile Ngcece, 214519385

Congratulations! Your doctoral research proposal titled An exploratory study of the South African Police Services (SAPS) systems in combating cybercrime, presented on 29 April 2021, has been accepted, without any corrections or revisions, by the Doctoral Research Proposal Review Panel of the School of Applied Human Sciences.

You are required to contact your supervisor for guidance on the next steps with your doctoral studies.

Yours faithfully

[redacted]

Ms Priya Konan
Postgraduate Officer
School of Applied Human Sciences

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

APPENDIX iv: Ethical Clearance Approval

12 November 2021

Slindile Ngcece (214519385)
School Of Applied Human Sc
Howard College

Dear S Ngcece,

Protocol reference number: HSSREC/00003010/2021
Project title: An Exploratory Study of the South African Police Services (SAPS) Systems in Combating Cybercrime
Degree: PhD

Approval Notification – Expedited Application

This letter serves to notify you that your application received on 22 June 2021 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted **FULL APPROVAL**.

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

This approval is valid until 12 November 2022.
To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be submitted when study is finished.

All research conducted during the COVID-19 period must adhere to the national and UKZN guidelines. HSSREC is registered with the South African National Research Ethics Council (REC

[redacted]

Yours sincerely,

Professor Dipane Hlalele (Chair) /dd

APPENDIX V: Gatekeeper Approval Letter

South African Police Service | Suid-Afrikaanse Polisiediens

Privaatsak Private Bag X94	Pretoria 0001	Faks No. Fax No.	(012) 393 2128

Your reference/U verwysing:

My reference/My verwysing: **3/34/2**

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

Enquiries/Navrae: **Lt Col Joubert**
AC Thenga
Tel: **(012) 393 3118**
Email: [redacted]

APPROVED

Ms S Ngcece
UNIVERSITY OF KWAZULU-NATAL

RE: PERMISSION TO CONDUCT RESEARCH IN SAPS: AN EXPLORATORY STUDY OF THE SOUTH AFRICAN POLICE SERVICES (SAPS) SYSTEMS IN COMBATING CYBERCRIME: UNIVERSITY OF KWAZULU-NATAL: DOCTORATE DEGREE: RESEARCHER: S NGCECE

The above subject matter refers.

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

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

The National Head: Directorate for Priority Crime Investigation:

- **Contact Person:** Brigadier M Mohajane
- **Contact Details:** [redacted]
- **Email Address :** [redacted]

The National Head: Directorate for Priority Crime Investigation has stressed that the researcher must provide a copy of the research report to the Directorate for Priority Crime Investigation.

Kindly adhere to paragraph 6 of our attached letter signed on the **2021-08-19** with the same above reference number.

[redacted]

MAJOR GENERAL
THE HEAD: RESEARCH
DR PR VUMA

DATE: 2021-10-21

APPENDIX Vi: Editors Letter

DR. KWAME OWUSU-AMPOMAH

{BA (Ed); MA (Cum Laude); D. Admin.}

RESEARCH AND DEVELOPENT STRATEGY CONSULTANT

14 Kirriemuir 59 Kennard Rise, Carrington Heights, Durban 4001

Dear Sir/Madam **28th January, 2025**

TO WHOM IT MAY CONCERN

This is to certify that I, the undersigned, have edited the Ph.D. Thesis of Ms. Slindile Ngcece, (Student Number: 214519385), titled **An Exploratory Study of the South African Police Services (SAPS) Systems in Combating Cybercrimes.**

Yours Sincerely

……

Dr. K. Owusu-Ampomah