JCSS Journal of Cyberspace Studies
eISSN: 2588-5502
http://jcss.ut.ac.ir
University of Tehran

Exploring Responses to Cybercrime in South Africa: The South African Police Services (SAPS) Perspectives

Slindile Ngcece[1], Sazelo Mkhize[2], Khanyisile Majola[2*]

1. Department of Humanities, School of Applied Human Sciences, University of Kwa Zulu Natal, KwaZulu-Natal, South Africa.
2. Department of Criminology and Security Science, School of Criminal Justice College of Law, The University of South Africa (UnISA), Pretoria, South Africa.

(*Corresponding author: ✉majola.berlinda@gmail.com, https://orcid.org/0000-0002-1247-4524)

Article Info

Review article

Main Object: Humanities & Social sciences, Cyber criminology

Received: 13 May 2025
Revised: 14 July 2025
Accepted: 14 July 2025
Published online: 25 July 2025

Keywords:
cybercrimes,
cybersecurity,
law enforcement,
policies,
South African police services.

Abstract

Background: The rapid development of technology and computing has significantly impacted modern societies, leading to increased opportunities for wealth creation and, inversely, transactional offending. Cybercrimes are increasing and have become a major threat to nations, governments, businesses, and individuals, resulting in financial losses, reputational damage, and personal information data breaches.
Aims: This study explores how the South African Police Service (SAPS) responds to and combats cybercrimes.
Methodology: This research was conducted in Durban, KwaZulu-Natal. The study adopted the qualitative research approach and the phenomenological research design, according to which interpretive and constructivist qualitative research paradigms were deemed appropriate. 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 orientation that guided the study is the Structural Functionalism Theory. Data were analyzed using thematic analysis.
Findings: The study revealed that South Africa has been experiencing an increase in cybercrimes. However, has introduced laws and security strategies, such as the Cybercrime and Cybersecurity Bill of 2017, to respond to cybercrimes. However, these are argued to be not adapting fast enough to the constantly changing technological environment.
Conclusion: Although limited, there are Police forensic experts in the field who can respond to cybercrimes. The study emphasizes the need for collaboration among all stakeholders, including prosecutors, the judiciary, private security agencies, CSPs, and ISPs, to effectively tackle cybercrimes.

Cite this article: Ngcece S, Mkhize S, Majola K. (????). "Exploring Responses to Cybercrime in South Africa: The South African Police Services (SAPS) Perspectives". *Cyberspace Studies*. ?(?): 1-21. doi: https://doi.org/10.22059/jcss.2025.395262.1149.

Website: https://jcss.ut.ac.ir/| Email: jcss@ut.ac.ir |
EISSN: 2588-5502
Publisher: University of Tehran

Cyberspace Studies, Vol ?, No ?, ????

1. Introduction

According to Gumbi (2018), and Mabunda (2021), internet connectivity in Africa has significantly increased. 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 et al., 2024). This study explores how law enforcement agencies, specifically SAPS, have responded to the staggering increase of cybercrimes in South Africa. 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. Fraudsters and cybercriminals continue to capitalize on the expansion of broadband access and technological advancements, committing their crimes at huge costs to the state, corporate bodies, and individuals.

1.1. The prevalence and Trends of cybercrimes

Globally, cybercrime leads to financial losses, reputational damage, and personal information data breaches. 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 was the outbreak of the COVID-19 pandemic (*IBM*, 2024). South Africa is indeed not an exception to the growing cybercrime challenges. In 2016, South Africa is estimated to have lost US$242 million; the estimates also show that the country loses US$157 million annually to cybercrime. While in 2018, the country was ranked among the top ten countries in Africa with regard to cyber-attacks (Mabaso, 2018), it has since not had a safe space from cyber threats. It is worth noting, however, that developments in cyberspace indicate that considerable efforts are being made in Africa to combat and respond to cybercrimes. The government of South Africa, for instance, has taken steps to enact cybercrime laws (Gumbi, 2018). The Cybercrimes Bill is South Africa's first legislative response to cybercrime, following the Electronic Communication and Transactions Act (ECTA) enacted in 2002. International and regional cybercrime policies, such as the Council of Europe Convention on Cybercrime and the African Union Convention on Cybersecurity and Personal Data Protection, have also been developed to respond to cybercrimes. However, 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).

1.2. Cybercrime polices in South Africa

The South African Police Service (SAPS), like all other law enforcement agencies 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 Cybercrimes 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).

1.3. 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 et al., 2021). The objectives of the bill provide that the executive may negotiate with foreign states to promote cyber security and 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, and create cybercrime offenses **(**ibid).

The Bill further mentions the following as cybercrimes committed unlawfully and intentionally (Boda et al., 2021; Mtuze & Musoni, 2023).

S2. 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).

S3. Unlawful interception of data (acquisition, viewing, capturing, copying)

S4. Unlawful acts in respect of software and hardware tools (use or possess)

S5. 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).

S7. Unlawful acquisition, possession, provision, receipt, or use of password, access codes, or similar data or devices (purpose)

S8. 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).

S9. 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).

S11. 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).

S12. 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)

Malicious communications include:

S14. Data message that incites damage to property or violence.

S15. Data message that threatens persons with damage to property or violence

S16. Data message of intimate image

1.4. Powers to investigate, search, and access/seize

All criminal investigations start with the Criminal Procedure Act (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. A broad range of procedural authorities is particularly provided for police officials in Chapter 5 of the Bill (Reddy, 2019). 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) (ibid). Standard Operating Procedures are also provided under the Cybercrimes Bill, specifically for acquiring and storing electronic evidence. 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 (ibid). Bringing criminals to justice depends on the powers of the South African police service (SAPS) and the Minister of State Security.

1.5. South African Police Services (SAPS) in policing the Cybercrimes Bill

The South African Police Service (SAPS) is committed to providing a secure information technology environment for all citizens (Boda et al., 2021). As a national law enforcement entity, SAPS is required to adopt measures and strategies to combat cybercrime (Kempen, 2019). Through the Cybercrimes Bill, Chapter 10, Section 54, the government must ensure the police service has sufficient human and operational capacity to detect, prevent, and investigate cybercrimes, and develop accredited training programs. 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. 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).

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

The Electronic Communications and Transactions Act (ECT) 25 of 2002 is among the legislation that was enacted in response to the ineffectiveness of South African common law in combating cybercrime. Currently, the ECT Act's criminal legislation provisions serve as the primary statutory defence against cybercrime in South Africa. 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). 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, 2022).

1.7. 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. It seeks to protect information and data by addressing the issues of security, discrimination, and theft (Ralarala, 2020). 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. 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 (ibid). 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).

1.8. 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 safe and reliable cyber environment (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 (ibid).

1.9. 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 with the pace at which 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 et al., 2020). Indeed, van Vuuren et al. (2020) state 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 et al., 2022).

Cyberspace Studies, Vol ?, No ?, ????

1.10. 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 et al., 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 et al. (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 et al., 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, preservation, gathering, analysis and presentation of digital evidence. 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 requires certain equipment, methods, and knowledge (Kazaure et al., 2023).

1.11. Methods and Instruments in scientific evidence

1.11.1. 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. 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, Jantan and Yusoff (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.

1.11.2. Analysing data/ Evidence

Cybercrimes like cyberbullying and defamation on social media have been identified using sentiment analysis and natural language processing. Detection systems combine keyword analysis with user behavior to identify hostile conduct. Social media monitoring methods are also used to track illicit behavior on platforms like Facebook and Twitter. The complexities of online environments make gathering and examining social media data crucial (Kazaure et al., 2023).

1.12. 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 before the cybercrime incident. It suggests that cybercrime measures and evidence collected before the crime occurs can be implemented. 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. Behavioral biometrics offers a method for producing behavioral characteristics of digital artifacts to allow for their forensic preservation for digital investigation (ibid).

According to Al-Dhaqm et al. (2021), this method is becoming more widely used in digital forensics. Behavioral 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

behavioral 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 et al., 2020). Mugisha (2019) further mentions several specialized branches in digital forensics that deal with cybercrimes. Namely the Disk Forensics**.** Disk forensics, Printer Forensics, Network Forensics, Mobile Device Forensics, Database Forensics, and Personal Digital Assistant (PDA) Forensics

1.13. Recent development in cybercrime responses

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 et al., 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 (ibid).

In recent years, multi-factor authentication has become more popular, requiring users to submit various kinds of authentication (Kazaure et al., 2023; Vitus, 2023; Chudasama et al., 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 et al., 2023).

1.14. Structural Functionalism Theory

This study utilized Structural Functionalism Theory, a 1930s writing by Parsons and Merton, which asserts that society is composed of interdependent systems that cannot function without each other (Olayemi, 2014). The functional structural approach aims to create social order and balance by integrating members based on shared principles, norms, and beliefs. This approach views society as a functionally integrated system, with any malfunction impacting the organism's life (Pasaribu et al., 2018; Enweonwu et al., 2021).

Robert K. Merton's Structural-Functionalist School of Thought posits that social patterns, institutions, and structures have both manifest and latent functions, addressing unintended, unplanned, neglected, and unfamiliar consequences (Abdul-Rasheed et al., 2016). Technology development aimed at social and economic development has led to cybercrimes. Structural functionalism theory suggests that interconnected family, education, government, police, and economy elements are interdependent, affecting social structure. Issues like crime, unemployment, poverty, and social influence affect the effectiveness and efficiency of society (Alabi et al., 2023). Alabi et al. (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 & 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. Moreover, according to Rustad (2001), 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. Kempen (2019) further argues that 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. The country still lacks the knowledge and expertise in the cyber field.

2. Methodology

This study employed a qualitative research approach to explore the subjective opinions, experiences, and views of police officers on cybercrimes in South Africa. Seventeen participants were purposively selected from the KwaZulu Natal provincial SAPS office in the Durban metropolitan area, with fourteen (n14) from the Durban Commercial Crimes Unit and three (n3) from the Directorate for Priority Crime Investigation (DPCI). The police officers were selected based on their availability, willingness to participate in the study, and experience in dealing with cybercrime cases. In-depth face-to-face interviews were conducted with participants to gather data, which were audio-recorded with their permission. Thematic analysis was used to analyze the data,

involving the identification of recurring themes, codes, and patterns. The researcher ensured the accuracy and confidentiality of the data, using pseudonyms to protect participants' identities. Ethical clearance was obtained from the Humanities and Social Sciences Research Ethics Committee (HSSREC), and a gatekeepers' letter was secured from the South African Police Services (SAPS) research office. Participation was voluntary, and informed consent was obtained from all participants.

3. Findings

The data generated themes related to understanding and combating cybercrimes in South Africa.

3.1. Roles of the South African police officers in the DPCI and commercial crimes unit

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. 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"
>
> **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 showed they had the ability and skill to respond to online crimes. The findings further confirm 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).

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).

> **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 (Kempen, 2019). By having these units and experts, SAPS further addresses its constitutional obligation to adopt measures, policies, and/or strategies to deal with cybercrime.

3.2. Police officers' views on cybercrimes in South Africa

This sub-theme aimed to understand and demonstrate participants' views about cybercrimes 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."

It was evident that the common perspective for all interviewed participants is that cybercrimes are on the rise in South Africa. 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 are unaware of online crimes and their severity. 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 of cybercrimes or how to protect themselves from them. Invariably, cybercriminals target the unprepared, who easily fall prey to the dangers of online crimes.

Participant 16 shared views as follows:

> **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 as 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."

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.

> **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 occurs as a result of structural failure, which makes bringing about stability in cyberspace a challenge for law enforcement officers (Rustad, 2001).

3.3. 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) states 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. The study revealed that although participants were in the same line of work and investigating cybercrimes, their roles in responding to cybercrimes in the department differed slightly. 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, a digital forensic investigator 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."

P6. "There is a 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. 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."

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 a crime has occurred and prosecute offenders. Al-Dhaqm et al. (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. In most cases, this procedure enables them to access very useful confidential information. 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 and operate 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 et al. (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 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 et al., 2021). In this instance, laws must be communicated and shared for effective implementation and investigation.

4. Discussion

The study indicated that cybercrimes are indeed a challenge in South Africa. Evidently, considerable efforts are being made in South Africa to reduce or eliminate cybercrime and its impact. The study found that the SAPS forensic unit is charged with the responsibility of dealing with cybercrimes in South Africa. In responding to cybercrimes, the participants mentioned Section 205 of the Criminal Procedure Act 51 of 1977 as an act or guideline they use in fighting against cybercrimes. They also engage in local and international collaboration in the investigation of cases and the arrest of offenders. They also engage in the retrieval and analysis of digital data from computers and other digital devices. The retrieved digital data, as digital evidence, is then presented in court in the prosecution of arrested cybercrime offenders. However, although considerable measures or cyber instruments have been put in place to reduce or eliminate cybercrime, the phenomenon has been increasing. The increasing trend of cybercrime incidents, and the fast pace of technological change and the modus operandi of cybercriminals complicate the already challenging law enforcement environment, making the work of digital forensic experts arguably more difficult

5. Conclusion

The focus of this study was to explore how South Africa, specifically law enforcement agencies (the SAPS), respond to and combat cybercrimes. 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. Cybercrime is not only a national but also a worldwide concern, and at both levels may be understood from the perspectives of the structural functionalist theory. In that regard, combating 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 and individuals.

Conflict of interest

The authors declared no conflicts of interest.

Ethical considerations

The authors have completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc. This article was not authored by artificial intelligence.

Data availability

The dataset generated and analyzed during the current study is available from the author on reasonable request.

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

References

Abdul-Rasheed, S.L.; Lateef, I.; Yinusa, M.A. & Abdullateef, R.A. (2016). "Cybercrime and Nigeria's external image: A critical assessment". *Africology*: *The Journal of Pan African Studies*, 9(6). https://www.jpanafrican.org/docs/vol9no6/9.6-9-Abdual-Rasheed.pdf.

Alabi, A.; Bamidele, A.H. & Oladimeji, A.B. (2023). "Cybercrime in Nigeria: Social influence affecting the prevention and control". *Lafia Journal of Economics and Management Sciences.* 8(1). https://www.lajems.com/index.php/lajems/article/download/249/194.

Al-Dhaqm, A.; Ikuesan, R.A.; Kebande, V.R.; Razak, S.; Grispos, G. & Choo, K.R (2021). "Digital forensics subdomains: The state of the art and future directions". *IEEE Access*. 9. https://doi.org/10.1109/ACCESS.2021.3124262.

Bankole, F.; Taiwo, A. & Claims, I. (2022). "An extended digital forensic readiness and maturity model". *Forensic Science International: Digital Investigation*. 40. https://doi.org/10.1016/j.fsidi.2022.301348.

Baror, S.O.; Ikuesan, R.A. & Venter, H.S. (2021). "A defined digital forensic criteria for cybercrime reporting". *17th International; Conference on Intellectual Capital, Knowledge Management & Organisational Learning*. http://dx.doi.org/10.34190/ICCWS.20.056.

Barrett, A.M. (2013). "Education and other sustainable development goals: a shifting agenda for comparative education". *Compare: A Journal of Comparative and International Education*. 43(6): 825-829. https://doi.org/10.1080/03057925.2013.850285.

Boda, R.; Dullabh, R. & 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).

Capazorio, S. & Hollis, R. (2017). From silk road to tor tunnels: A look at the history and development of cybercrimes". *Cybercrime Law Feature*. https://www.withoutprejudice.co.za/publication/2017/July/articles.

Chudasama, D.; Patel, D. & Shaikh, N. (2020). "Research on cybercrime and its policing". *American Journal of Computer Science and Engineering Survey.* 8(3): 14. https://www.imedpub.com/computer-science-and-engineering-survey.

Enweonwu, O.A.; Ugwu, I.P.; Onyejegbu, D.C.; Areh, C.E. & Ajah, B.O. (2021). "Religious fanaticism and changing patterns of violent crime in Nigeria". *International Journal of Criminology and Sociology*. 10: 1378-1389. https://doi.org/10.6000/1929-4409.2021.10.158.

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". *University of Cape Town*. http://hdl.handle.net/11427/29247.

Hofmeyr, C.D. (2020). "The Cybercrimes Bill is one step away from becoming law". *Technology, Media & Telecommunications Alert*. https://www.cliffedekkerhofmeyr.com/export/sites/cdh/news/publications/2020/technology/downloads/Technology-Media-Telecommunications-ALert-7-July-2020.pdf.

IBM. (2024). "Cost of a data breach report". https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf (Accessed 10 December 2024).

ITU: 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).

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*. 11(4): 14-39. https://doi.org/10.1633/JISTaP.2023.11.4.2.

Kempen, A. (2019). "Fighting cybercrime requires an integrated and international effort- The SAPS's envisaged approach". *Servamus Community-Based Safety and Security Magazine*. 112(1). https://hdl.handle.net/10520/EJC-130abd8806.

Kuzior, A.; Tiutiunyk, I.; Zielińska, A. & Kelemen, R. (2024). "Cybersecurity and cybercrime: Current trends and threats". *Journal of International Studies*. 17(2): 220-239. https://doi.org/10.14254/2071-8330.2024/17-2/12.

Lourie, G. (2015). "What is South Africa doing to reduce cybercrime—tech financials". *Tech* Financials. https://www.techfinancials.co.za/2015/11/05/what-sa-is-doing-to-reduce-cybercrime/.

Mabaso, J. (2018). *Assessing the Cyber-Security Status of the Metropolitan Municipalities in South Africa*. College of Law & Management Studies, University of KwaZulu-Natal. https://researchspace.ukzn.ac.za/handle/10413/18097.

Mabunda, S.M. (2021). *The South African Legislative Response to Cybercrime*. PhD Thesis, University of the Western Cape.

Maluleke, W. (2023). "Exploring cybercrime: An emerging phenomenon and associated challenges in Africa". *International Journal of Social Science Research and Review*. 6(6): 223-243. http://dx.doi.org/10.47814/ijssrr.v6i6.1360.

Mtuze, S.S. & Musoni, M. (2023). "An overview of cybercrime law in South Africa". *International Cybersecurity Law Review*. 4: 299-323. https://doi.org/10.1365/s43439-023-00089-8.

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). https://www.researchgate.net/publication/331991596_ROLE_AND_IMPACT_OF_DIGITAL_FORENSICS_IN_CYBER_CRIME_INVESTIGATIONS.

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*. 36(2). https://doi.org/10.25159/2522-6800/8112.

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. https://doi.org/10.5897/IJSA2013.0510.

Pandey, A.K.; Tripathi, A.K.; Kapil, G.; Singh, V.; Khan, M.W.; Agrawal, A.; Kumar, R. & Khan, R.A. (2020). *Current Challenges of Digital Forensics in Cyber Security*. IGI Global Scientific Publishing. http://dx.doi.org/10.4018/978-1-7998-1558-7.ch003.

Pasaribu, R. (2018). "Fight narcotics with community strengthening: Crime control management by community policing". *Journal of Indonesian Legal Studies*. 3(2): 237-252. https://doi.org/10.4018/978-1-7998-1558-7.ch003.

Ralarala, S. (2020). *The Impact of Cybercrime on e-Commerce and Regulation in Kenya, South Africa, and the United Kingdom*. Master thesis. School of Law, Strathmore University. https://su-plus.strathmore.edu/server/api/core/bitstreams/d2089a73-0980-4b48-8f81-36a592e399d8/content.

Reddy, E. (2019). "Analysing the investigation and prosecution of cryptocurrency crime as provided for by the South African Cybercrimes Bill". *Statute Law Review*. 41(2): 1-14. http://dx.doi.org/10.1093/slr/hmz001.

Richards, N.U. & 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*. 35(2): 131-161.

https://doi.org/10.1080/13600869.2021.1885105.

Rustad, M.L. (2001). "Private enforcement of cybercrime on the electronic frontier". *Southern California Interdisciplinary Law Journal*. 11:63.

van Vuuren, J.C.; Leenen, L. & Pieterse, P. (2020). "Development and implementation of cybercrime strategies in Africa with specific reference to South Africa". *Journal of Information Warfare*. 19(3): 83-101. https://www.jstor.org/stable/10.2307/27033634.

Vitus, N.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*. 10(9). http://dx.doi.org/10.6084/m9.figshare.24155610.v1.

Wang, S.K.; Hsieh, M.; Chang, C.K.; Jiang, P. & 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*. 65(4). https://doi.org/10.1177/0306624X20952391.

Wu, T.; Breitinger, F. & O'Shaughnessy, S. (2020). "Digital forensic tools: Recent advances and enhancing the status quo". *Forensic Science International: Digital Investigation*. 34. https://doi.org/10.1016/j.fsidi.2020.300999.