This paper was presented at the 21st International Conference on Sustainable Development, held at the Faculty of Social Science and Humanities, University of Ottawa, Ottawa, Canada, on July 15-16, 2025

Evaluating the Role of the South African Police Service in Enforcing the Cybercrimes Act: Effectiveness and Challenges in Combating Cybercrime

Mmabatho Portia Aphane
Department: Police Practice, School of Criminal Justice, College of Law,
University of South Africa, Pretoria, South Africa.
Corresponding author: aphanmp@unisa.ac.za

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

Abstract: This study evaluates the role of the South African Police Service (SAPS) in enforcing the Cybercrimes Act No. 19 of 2020, focusing on its effectiveness and the challenges faced in combating cybercrime. This research utilises the desktop study approach and synthesises existing literature, reports, and data to provide a comprehensive analysis of SAPS efforts in this domain. The Cybercrimes Act No. 19 of 2020 was enacted in 2020 for the particular purpose of addressing the growing threat of cybercrime in South Africa by providing a legal framework for the identification, investigation, and prosecution of cyber offences. Despite the legislative advancements, SAPS faces significant challenges in implementing the Act effectively. These challenges include a lack of specialised skills and resources, insufficient training programmes, and the rapid evolution of cyber threats that outpace legislative and enforcement capabilities. One of the primary challenges identified is the shortage of specialised skills within SAPS. Cybercrime investigations require a unique set of technical skills and knowledge, which many officers currently lack. This skills gap is exacerbated by the rapid pace of technological advancements, making it difficult for law enforcement to stay ahead of cybercriminals. Additionally, the limited availability of resources, such as advanced forensic tools and software, hampers the ability of SAPS to conduct thorough and timely investigations. Training programmes for SAPS officers are another critical area of concern. While there have been efforts to provide cybercrime training, these programmes are often insufficient in scope and depth. Many officers receive only basic training, which does not sufficiently equip them with the necessary skills to handle complex cybercrime cases. As such, there is a compelling demand for more comprehensive and continuous training programmes that cover the latest developments in cybercrime and cybersecurity. The study highlights the effectiveness of the SAPS's current strategies, such as the establishment of specialised cybercrime units and the development of Standard Operating Procedures (SOPs) for cybercrime investigations. These units are tasked with handling cybercrime cases and have shown some success in identifying and prosecuting offenders. The SOPs provide a structured approach to investigations, ensuring that cases are handled systematically and efficiently. However, the effectiveness of these strategies is limited by several factors, such as the lack of inter-agency collaboration. The research underscores the importance of continuous adaptation and innovation in law enforcement practices in order to keep pace with the dynamic nature of cybercrime. Cybercriminals are constantly developing new methods and techniques, requiring law enforcement to be agile and proactive in their response. This includes investing in new technologies, such as artificial intelligence and machine learning, which could enhance the ability to detect and prevent cybercrime. International cooperation is another critical aspect of effective cybercrime enforcement. Cybercrime is a global issue, and many cybercriminals operate across borders. The SAPS should engage in international collaborations and participate in global initiatives to combat cybercrime. This includes sharing information and best practices with other countries, as well as participating in joint operations for the apprehension of cybercriminals. In conclusion, this study provides valuable insights into the current state of the SAPS's enforcement of the Cybercrimes Act No. 19 of 2020, offering recommendations for addressing the identified challenges and improving the overall efficacy of cybercrime prevention and enforcement in South

Africa. The SAPS has made notable strides in combating cybercrime. However, there is compelling need for ongoing investment in training, technology, and international cooperation by the SAPS in order to enhance its organisational effectiveness. The SAPS can improve its ability to protect South Africa from the growing threat of cybercrime by addressing these challenges and leveraging the strengths of both the public and private sectors.

Keywords: Act, Challenges, Combating, Cybercrimes, Effectiveness, Enforcing, Evaluation, Role

Introduction

Cybercrimes emerging from the Fifth Industrial Revolution (5IR) pose a growing and complex challenge for South Africa and many other countries globally. The 5IR technologies have increasingly blended human-centric artificial intelligence, robotics, and interconnected systems, rendering the digital landscape more vulnerable to sophisticated cyber threats. While these innovations promise significant socio-economic benefits, they also introduce complex cybersecurity challenges, particularly for developing nations like South Africa. The integrated intelligence of digital infrastructures has simultaneously induced more vulnerability to sophisticated cyber threats. These threats are no longer confined to isolated incidents, but are increasingly systemic and target critical infrastructure, financial systems, and personal data at an unprecedented scale.

In the South African context, the rise in cybercrime is compounded by structural limitations within the country's law enforcement and cybersecurity ecosystems. The South African Police Service (SAPS), which bears the primary responsibility for enforcing the Cybercrimes Act No. 19 of 2020, faces significant hurdles in adapting to the rapidly evolving nature of cyber threats. These threats include the shortage of skilled personnel, limited access to advanced forensic tools, as well as deficient inter-agency coordination. The decentralised and often anonymous nature of cybercrime further complicates investigation and prosecution efforts, particularly in a legal environment still adjusting to the demands of digital evidence collection and cross-border cooperation (Nelufule, Masango, & Singano, 2024; Amoo et al., 2024).

Despite these challenges, SAPS has made notable strides in developing institutional responses to cybercrime. The establishment of specialised cybercrime units and the implementation of Standard Operating Procedures (SOPs) for digital investigations represent important steps toward professionalising cyber enforcement (Adula, Kant, & Birbirsa, 2023). However, the effectiveness of these measures remains uneven, particularly in the context of increasing criminal sophistication and public skepticism regarding law enforcement's capacity to deliver justice in the digital realm (Aphane & Mofokeng, 2021). Moreover, the symbolic strength of the Cybercrimes Act No. 19 of 2020 is often undermined by practical enforcement gaps, including under-reporting, digital illiteracy, and resource constraints (Mohammed et al., 2019; Pieterse, 2021).

This paper critically evaluates the effectiveness and limitations of the SAPS in combating cybercrime in terms of the Cybercrimes Act No. 19 of 2020, with particular focus on the implications of 5IR technologies. The paper explores the institutional, legal, and socio-technical dimensions of cybercrime enforcement in South Africa, drawing on recent case studies, policy reviews, and academic literature. By identifying both the successes and shortcomings of current strategies, the paper aims to contribute to a more nuanced understanding of the strategies and approaches by whose means South Africa could strengthen its cyber resilience in an increasingly digitalised and interconnected world.

Theoretical perspectives of cybercrime enforcement

Cybercrime, by its nature, challenges traditional criminological theories due to its borderless, anonymous, and technologically mediated characteristics. However, several theoretical frameworks remain relevant in understanding both the motivations for cyber offences and the strategies for their prevention and control. The deterrence theory, routine theory, and situational crime prevention theory were deemed both relevant and instructive for purposes of this paper.

Deterrence theory posits that individuals are less likely to commit crimes in the event that they perceive the consequences to be certain, swift, and severe (Apel, 2013). In the context of cybercrime, this theory underscores the importance of visible enforcement, effective prosecution, and public awareness of legal consequences. However, the low conviction rates and under-reporting of cybercrime in South Africa weaken the deterrent effect of existing laws (Aphane & Mofokeng, 2021). Moreover, the anonymity and transnational nature of cybercrime often reduce the perceived risk of apprehension, further undermining deterrence.

Routine activity theory suggests that crime occurs when a motivated offender, a suitable target, and the absence of a capable guardian converge in time and space (de Melo, Pereira, Andresen & Matias, 2017). Applied to cyberspace,

this theory highlights the need for digital guardianship — such as firewalls, encryption, and user education — to reduce opportunities for cyber offending. This theory also implies that law enforcement agencies such as the SAPS should act as capable guardians by actively monitoring, investigating, and prosecuting cyber offences (Van Niekerk & Maharaj, 2022). However, the lack of digital literacy among the public and limited cyber capabilities within the SAPS often leave digital spaces inadequately guarded.

Situational crime prevention theory focuses on reducing the opportunities for crime through environmental design and technological safeguards (Clark, 2018). In the digital realm, the focus on situational crime prevention includes measures such as secure coding practices, multi-factor authentication, and real-time threat detection systems. While these are primarily implemented by private sector stakeholders, law enforcement plays a critical role in promoting and supporting such practices through regulation and collaboration (Mohammed et al., 2019). However, the fragmented nature of cybersecurity governance and absence of a unified national incident response strategy in South Africa, limit the effectiveness of situational prevention efforts. These theoretical frameworks collectively underscore the importance of a multi-layered approach to cybercrime prevention — one that combines legal enforcement with technological, educational, and institutional interventions.

Literature review

A research literature review is a methodical, transparent, and repeatable process for identifying, evaluating, and synthesising the corpus of completed and documented work produced by researchers, academics, and practitioners (Fink, 2019). The groundbreaking work of scholars and researchers serves as the foundation for conclusions reached in a research review. Creswell (2014) further explains and bolsters the afore-mentioned assertion, emphasising that a literature review is a necessary component of any research report or thesis. Therefore, the literature review could include the following aspects: background data to prove the existence of a problem under investigation; research paradigms as a source of ontological and epistemological assumptions; theory of relevance to the "why" questions; and prior research on the subject or other related subjects.

The SAPS has made notable strides in combating cybercrime. However, there is a compelling need for ongoing investment in training, technology, and international cooperation to enhance the effectiveness of such strides. The SAPS can improve its ability to protect South Africa from the growing threat of cybercrime by addressing these challenges and leveraging the strengths of both the public and private sectors. Reconstructing a cybercrime scene and linking the perpetrators to the offence is extremely challenging for investigators (Ezeji, 2024). This difficulty largely stems from the jurisdictional complexities of cybercrime, in terms of which offenders often operate from different countries with different legal systems. These cross-border dynamics hinder timely cooperation between law enforcement agencies, complicate evidence collection, and renders the task of establishing a direct connection between the suspect and the cybercrime scene nearly impossible.

Cybercrime Act No. 19 of 2020

The Cyber Crimes Act, No. 19 of 2020 ("Cyber Crimes Act") was signed into law in June 2021, and officially came into effect on 1 December 2021 for the purpose of strengthening South Africa's legal framework against cybercrime (Atuguba, 2021). The Act criminalises a wide range of cyber activities, including unlawful access to data, cyber fraud, cyber extortion, and the distribution of malicious software. The Act also provides for the establishment of procedures for the investigation, search, seizure, and prosecution of cyber offences (Snail ka Mtuze, 2022). One of the Act's key strengths lies in its attempt to harmonise South African law with international standards, particularly those outlined in the Budapest Convention on Cybercrime. In that regard, the Act introduces mechanisms for international cooperation, including mutual legal assistance and the sharing of electronic evidence across borders. However, critics argue that the Act's implementation has been hampered by factors such as institutional fragmentation, limited public awareness, and a lack of technical capacity within SAPS and the judiciary (Bote, 2019). The Act grants South African law enforcement agencies broad investigative powers, including the ability to search and seize data from private networks, even without a warrant to do so in certain cases. The Act also imposes a legal duty on members of the public and certain institutions to report cybercrimes, with non-compliance possibly resulting in fines, imprisonment of up to 15 years, or both. Importantly, the Act extends the jurisdiction of South African courts to include cybercrimes committed outside the country in the event that such crimes affect individuals or businesses within South Africa. This international reach, combined with enhanced investigative powers, aims to close legal gaps that cybercriminals often exploit (South Africa, 2020).

In addition to its international focus, the Cyber Crimes Act aims at protecting individuals and businesses from the growing threats in the digital landscape. To that effect, the escalating rate of cyberattacks necessitates a thorough

examination of the SAPS's capacity to investigate and prosecute cybercrimes, given the dynamic nature of digital threats and the evolving methodologies of cybercriminals in particular (Aphane & Mofokeng, 2021). The pervasive nature of cybercrime is further evidenced by reports indicating that public sector institutions in South Africa frequently conduct cybersecurity risk assessments, with a significant proportion experiencing multiple cyber incidents annually (Henrico & Els, 2025). Although efforts have been made both nationally and internationally to address cybercrime, research shows that country-specific legal systems have not been completely successful in eliminating this issue (Rao & Pradhan, 2020). The problem is worsened by the lack of a shared definition of cybercrime. What is considered a crime in one country may not be viewed as such in another, allowing cybercriminals to evade prosecution. While the Cybercrimes Act provides a legal framework for enforcement, its implementation has been inconsistent across various South African provinces. It is in that regard that the National Cybersecurity Policy Framework (NCPF) intended to guide inter-agency collaboration and policy alignment, but criticised for its vague mandates and lack of operational clarity (Shingange, 2024). The latter state of affairs has resulted in the SAPS being often left to navigate complex cyber threats with limited support, as well as lack of a unified national strategy and clearly defined roles for stakeholders.

Mpahlwa (2025) argues that the Cybercrimes Act is emblematic of South Africa's establishment of a comprehensive legislative framework to combat cybercrime. This framework is further supported by related laws, including the Protection of Personal Information Act (POPIA), No. 4 of 2013 and the Electronic Communications and Transactions Act (ECTA), No. 25 of 2002. However, the existence of these legal instruments continues to pose a significant enforcement challenge. For instance, the country struggles to keep pace with the rapidly evolving tactics employed by cybercriminals, who continuously adapt their methods to exploit technological vulnerabilities and regulatory gaps. In that regard, Mpahlwa (2025) acknowledges that the enforcement of cybercrime laws in South Africa is hindered by a lack of specialised local enforcement agencies and limited digital forensic capacity. Consequently, South African law enforcement authorities often rely on international partners such as the Federal Bureau of Investigation (FBI) for intelligence and operational support. This dependency underscores the need for greater investment in local cybercrime units, training, and infrastructure. Furthermore, the transnational nature of cybercrime complicates jurisdictional issues, making it difficult to prosecute offenders who operate across national borders. Mpahlwa (2025) then concludes that South Africa's legal protections will remain largely theoretical and offer limited deterrence against the growing threat of cybercrime, due to the paucity of stricter enforcement mechanisms and enhanced inter-agency coordination.

Emerging cybercrime trends in the 5IR era

The Fifth Industrial Revolution (5IR) is transforming the global digital landscape by integrating human-centric technologies such as artificial intelligence (AI), robotics, and the Internet of Things (IoT) into everyday life (Ziatdinov, Atteraya & Nabiyev, 2024). These innovations offer significant benefits for economic growth and service delivery, and also introduce new vulnerabilities that cybercriminals are increasingly exploiting. In South Africa, the rapid adoption of 5IR technologies, often without corresponding investments in cybersecurity, has created unprecedented fertile ground for a new generation of cyber threats that are more sophisticated, targeted, and damaging. In this regard, one of the most prominent trends relates to the escalation of ransomware attacks, which have evolved from opportunistic campaigns into highly coordinated, targeted operations. The 2024 Sophos State of Ransomware Report revealed that the average ransom payment in South Africa reached R17.9 million, with recovery costs averaging R19.44 million — which excludes the ransom itself (Sophos, 2024). These attacks have affected both public and private institutions, with the National Health Laboratory Service (NHLS) suffering a breach in June 2024 that resulted in the theft of 1.2 terabytes of sensitive data (Cybersecurity Hub, 2025). Such incidents disrupt essential services, erode public trust, while also exposing systemic weaknesses in digital infrastructure. According to Singh (2024), the increasing use of AI by attackers to automate phishing, malware deployment, and vulnerability scanning has rendered traditional security measures less effective, necessitating the development of advanced detection tools and collaborative research platforms such as MalFE (Singh, 2024).

In addition to ransomware, phishing and social engineering attacks have become more prevalent, particularly those leveraging AI-generated content and deepfake technologies. These attacks are increasingly used to compromise financial systems, steal personal data, and gain unauthorised access to corporate networks. The rise of generative AI tools has made it easier for attackers to craft convincing fake emails, voice messages, and even video content, rendering detection more difficult and increasing the success rate of such scams (Wendt, 2024). South Africa's critical infrastructure and government systems have also been frequent targets. Between 2023 and 2025, cyberattacks were reported against the Department of Justice, the Government Employees Pension Fund (GEPF), and the South African National Defence Force (SANDF), among others (Cybersecurity Hub, 2025). These breaches often involve data exfiltration and ransomware, with attackers demanding cryptocurrency payment in order to avoid public disclosure.

The implications of such attacks extend beyond financial loss, threatening national security and undermining the credibility of State institutions. In its 2024 Risk Report, the Institute of Risk Management South Africa (IRMSA) identified cybercrime as one of the five foremost strategic risks facing the country. The afore-cited report emphasised further that South Africa's cybersecurity maturity remains low, compared to global standards. This was exemplified in the lack of skilled professionals, fragmented governance, and insufficient investment in cyber resilience (IRMSA, 2024). Based on these low performance indicators, the IRMSA then called for a more integrated approach to cyber risk management, including real-time threat intelligence sharing, cross-sector collaboration, and the development of a national cyber resilience strategy.

Institutional capacity and challenges facing SAPS

The SAPS plays a central role in enforcing the Cybercrimes Act and responding to the country's growing cyber threat landscape. However, the institution faces a range of structural, operational, and technological challenges that hinder its organisational effectiveness and capacity to combat cybercrime. In South Africa, the challenges posed by cyber threats are increasing, especially at time when we navigate the complexities of the Fifth Industrial Revolution (5IR). The rapid pace of technological advancement requires the law enforcement agencies to be both well-equipped and highly agile in addressing these sophisticated cyber threats. This means enhancing skills, resources, and coordination among various stakeholders to effectively protect citizens and institutions in a continuously evolving digital landscape. One of the most compelling issues in this regard, relates to the shortage of specialised skills within the SAPS. Despite the establishment of cybercrime units in major South African provinces, many officers still lack the technical training required to investigate and prosecute cyber offences more effectively. Amoo et al. (2024) note that the rapid evolution of cyber threats has outpaced the development of digital forensic capabilities within the SAPS, resulting in delayed investigations and low conviction rates. Such demonstration of the skills gap is further exacerbated by limited access to advanced forensic tools, outdated IT infrastructure, and insufficient funding for capacity-building initiatives. In addition to technical limitations, the SAPS also faces institutional and procedural challenges. The absence of a centralised cybercrime reporting and case management system has led to fragmented data collection and poor coordination between units. This fragmentation undermines the ability to track cybercrime trends, allocate resources efficiently, and respond to incidents in a timely manner. Moreover, the lack of standardised protocols for handling digital evidence often results in procedural errors that compromise the admissibility of evidence in court (Adula, Kant & Birbirsa, 2023). Despite these challenges, there have been some positive developments. For instance, the introduction of Standard Operating Procedures (SOPs) for cybercrime investigations has helped to formalise investigative processes and improve case handling. In addition, the SAPS has initiated more active engagement with private sector partners and civil society organisations to enhance its cyber capabilities. However, these efforts are still embryonic and require sustained investment, political will, and institutional reform for meaningful impact.

Similar to many other countries worldwide, South Africa faces a growing and complex challenge in addressing transnational cybercrime. Cybercriminals often operate across borders, with victims and perpetrators located in different jurisdictions, which complicates investigations and undermines the effectiveness of law enforcement responses. To that effect, Ngcece and Mkhize (2023) explain that cybercrime is not confined to geography or time zones. Accordingly, the digital evidence required to pursue such cases is often stored in foreign jurisdictions, which renders access difficult and time-consuming. Criminal activities may become widely spread across the globe in both time and space. Such a situation could render the investigation ineffective, because the victim and offender may not reside in one country, and the evidence needed to continue with the investigation may be found in another country. Moreover, the evolving tactics used by cybercriminals make it difficult for existing legal frameworks to keep abreast of measures such as identifying the modus operandi of the cybercriminals. South Africa's ability to respond effectively to cybercrime remains limited in the event that issues such as adequate resources, cross-border collaboration, and technical expertise are not addressed. The South African government continues to address these challenges through legislative measures such as the Cybercrimes Act, which criminalises a wide range of cyber offences, including unlawful access, data interference, cyber fraud, and the dissemination of harmful data messages (South Africa, 2020). This Act also provides for extra-territorial jurisdiction, which enables South African courts to prosecute offences that impact adversely on national interests, irrespective of their commission outside the country. However, the successful enforcement of this legislation is heavily reliant on the operational capacity of the SAPS and the strategic oversight of the Minister of State Security.

Notwithstanding progress in the legislative realm, enforcement still constitutes a significant concern. In that regard, the Institute for Digital Security and Innovation (2024) reports that South Africa's cybersecurity infrastructure is underdeveloped, with limited investment in digital forensic capabilities and a shortage of skilled personnel. These limitations significantly weaken the ability of the SAPS to investigate and prosecute cyber offences effectively.

Similarly, the Press Council of South Africa (2024) stresses that the robustness of the legal framework is impaired by its implementation deficit, which requires stronger collaboration between government departments, the private sector, and international partners. South Africa risks falling behind in its ability to effectively respond to the evolving threat landscape of cybercrime without such coordinated efforts. The lack of a centralised national cybersecurity strategy and the absence of a dedicated cybercrime unit within the SAPS further exacerbate the problem. These institutional gaps delay response times and also reduce public confidence in the State's ability to protect citizens from digital threats. Failure to address these challenges through sustained investment, skills development, and inter-agency cooperation exposes South Africa to the risk of further deterioration in its capacity to respond to the increasingly sophisticated and transnational nature of cybercrime.

Despite the rapid increase in cybercrime and its growing integration into everyday life, a significant challenge persists, with victims of cybercrime considerably less likely to report their victimisation to the police, compared to victims of traditional crimes (Aphane & Mofokeng, 2020). This under-reporting is largely attributed to deficient public trust in law enforcement agencies' ability to investigate and prosecute cyber offences effectively. Many South African police units remain under-resourced and lack personnel with the required technical expertise for managing complex digital investigations. According to Pieterse (2021), the country's expanding digital landscape has increased its vulnerability to cyber threats. However, the response capacity of law enforcement has not kept pace with the sophistication of cybercriminals. The implementation and investigation of cybercrime cases is further complicated by the advanced and often trans-national nature of these offences, which require time-intensive processes and cross-border cooperation. The dynamic and decentralised structure of digital networks also exacerbates the tracing of perpetrators and collection of admissible digital evidence. As highlighted by the Press Council of South Africa (2024), the effectiveness of the Cybercrimes Act depends on its legal provisions and robust enforcement, technological readiness, and collaboration between the public and private sectors. While cybercrime appears impossible to eliminate, vital strategies for mitigating its impact could be applied by raising public awareness, improving digital literacy, building institutional capacity, and encouraging greater cooperation between the public and law enforcement agencies.

Public trust and underreporting of cybercrime

Public trust in the SAPS also remains a significant barrier to effective cybercrime enforcement in South Africa. One of the most significant barriers in this regard, relates to the persistent under-reporting of incidents by victims. Despite the growing prevalence of cybercrime, many individuals and organisations remain reluctant to report their experiences to the SAPS. This under-reporting skews national cybercrime statistics, and also limits the SAPS's ability to develop proactive strategies based on accurate threat intelligence. Aphane and Mofokeng (2021) intimates that rebuilding public confidence will require greater transparency, improved communication, and demonstrable success in cybercrime investigations. The reluctance by the stakeholders concerned is primarily driven by a lack of public confidence in SAPS's ability to investigate and resolve cyber-related offences effectively. Aphane and Mofokeng (2020) further found that cybercrime victims are far less likely to report their victimisation than victims of traditional crimes, citing concerns about the technical capacity and responsiveness of law enforcement. In addition to the institutional credibility deficit, the general public's limited awareness of cybercrime reporting mechanisms contributes to the low rate of disclosure. Many victims are unaware of either the place or mechanisms to report cyber incidents, and even fear that reporting such crime will not lead to meaningful outcomes. To address this gap, platforms such as Cybercrime.org.za have been established to provide accessible information and guidance on recognising, preventing, and reporting cybercrime. These initiatives are aimed at empowering citizens and promoting a culture of cyber vigilance, but their reach and impact remain limited without broader public engagement and institutional support. The Press Council of South Africa (2024) has also emphasised the importance of public-private collaboration and community education in strengthening the enforcement of the Cybercrimes Act. It is the contention of the Press Council that the success of the Act depends on legal provisions, public trust, international cooperation, and the active participation of civil society. Without these elements, the gap between legislative intent and enforcement outcomes will persist, leaving many cybercrimes unreported and unresolved.

Ngcece and Mkhize (2023) revealed that the SAPS continues to struggle with adapting to the rapidly evolving nature of cybercrime. Despite the introduction of the Cybercrimes Act and related policy frameworks, the SAPS's response remains fragmented and largely reactive, with limited coordination between units and insufficient digital forensic capabilities. The current study highlights that many officers lack the specialised training required to investigate complex cyber offences, leading to delays in case resolution and further discouraging victims from reporting these crimes. Moreover, the criminal justice system as a whole has yet to fully grasp the complexities of technology-facilitated crimes, resulting in inconsistent prosecutions and a lack of precedent-setting judgments that could guide future enforcement efforts. The 2024 INTERPOL African Cyberthreat Assessment Report further underscores the

urgency of strengthening national cyber resilience. The report notes that South Africa remains one of the most targeted countries on the continent, with ransomware, business email compromise, and digital extortion among the most prevalent threats. However, the report is also indicative of a growing gap between countries that are cyber resilient, and those that are not. The gap is driven largely by disparities in digital infrastructure, public awareness, and institutional capacity. In South Africa's case, this gap is particularly evident in rural and under-served communities, where limited internet access and low digital literacy rates hinder both prevention and reporting. Addressing these disparities requires a holistic approach that includes legal reform and law enforcement training, sustained investment in public education, digital inclusion, and cross-sector collaboration.

Evaluation of SAPS strategies and interventions

In response to the growing threat of cybercrime, the SAPS has implemented several strategies aimed at improving its investigative capacity and aligning its operations with the provisions of the Cybercrimes Act. While these efforts represent important steps toward institutional reform, their effectiveness is mixed, with notable successes in some areas and persistent challenges in others. One of the most significant developments has been the establishment of specialised cybercrime units within the SAPS. These units are tasked with investigating cyber offences, conducting digital forensic analysis, and supporting provincial police stations in handling cyber-related cases. According to Adula et.al (2023), these units have contributed to improved case handling and successfully assisted in the identification and apprehension of cybercriminals in several high-profile cases. However, their reach is still limited, with many rural and under-resourced areas lacking access to such specialised support. The introduction of SOPs for cybercrime investigations has also enhanced procedural consistency. These SOPs provide a structured framework for evidence collection, chain of custody, and digital forensic analysis, helping to reduce procedural errors and improve the admissibility of evidence in court. Nonetheless, the implementation of SOPs has been uneven across provinces, often due to disparities in training, resources, and institutional support (Amoo et al., 2024).

The SAPS has also made efforts to engage with external stakeholders, including private sector cybersecurity firms, academic institutions, and civil society organisations. These partnerships have facilitated knowledge sharing, joint training initiatives, and the development of early warning systems. For example, the SAPS has collaborated with platforms such as Cybercrime.org.za for the purpose of promoting public awareness and providing guidance on reporting of cybercrime incidents. While these initiatives are promising, their impact is limited by low public engagement and a lack of sustained funding (Press Council of South Africa, 2024). Another area of progress relates to the integration of cybercrime enforcement into broader national security strategies. The SAPS has initiated participation in inter-agency task forces and contribution to national cybersecurity exercises aimed at testing response capabilities and improving coordination. However, these efforts are still nascent and require stronger leadership, clearer mandates, and more robust evaluation mechanisms to ensure long-term effectiveness (Shingange, 2024). Despite these initiatives, there are still key gaps that require amelioration. For instance, the lack of a centralised cyber incident reporting system continues to hinder data collection and intelligence sharing. Moreover, the absence of a national cybercrime database limits the ability to track repeat offenders, identify patterns, and allocate resources strategically. These shortcomings are reflective of the need for a more integrated, technology-facilitated, and data-driven approach to cybercrime enforcement in order to foster inter-agency collaboration and prioritises public trust.

Methodology

This study employed a qualitative desktop research approach in its evaluation of the role of the South African Police Service in enforcing the Cybercrimes Act and addressing the challenges associated with cybercrime in the context of the Fifth Industrial Revolution (5IR). Desktop research, also known as secondary research, involves the collection, review, and synthesis of existing data, literature, and official reports to draw insights and conclusions without conducting primary fieldwork (Bassot, 2022). Qualitative methods allow for a nuanced understanding of the operationalisation of legislation within law enforcement structures and the practice-related challenges that exist (University of Cape Town, 2024). The primary method of data collection was a desktop-based literature review. The study focused on synthesising information from a variety of credible sources, including the following:

- Peer-reviewed academic journals on cybercrime and policing in South Africa.
- Government publications and policy documents, such as the Cybercrimes Act No. 19 of 2020 and the National Cybersecurity Policy Framework (NCPF).
- Reports from oversight bodies and civil society organisations, including the Press Council of South Africa and the Institute of Risk Management South Africa (IRMSA).
- News articles and case studies detailing recent cybercrime incidents and SAPS responses.

- International literature on cybercrime enforcement and best practices.

Sources were selected on the basis of their relevance, credibility, and recency, with particular focus on publications from the past five years to ensure the data reflects current practices and developments. Through a conceptual and critical evaluation of selected scholarly literature, this study provides valuable insights into the role of the SAPS in enforcing the Cybercrimes Act with specific attention on its effectiveness; as well as the challenges faced in combating cybercrime. The article adopted a qualitative systematic review as its primary methodological approach, due to its capacity to provide an in-depth and profound analysis of the SAPS's role in enforcing the Cybercrimes Act. This method was intended to yield in-depth insights into the effectiveness and challenges of law enforcement in the cybercrime domain. As a desktop study, this research is limited by its reliance on secondary data. The absence of primary data collection (e.g., interviews with SAPS officials or cybercrime victims) could further limit the depth of insight into operational realities. The researcher encountered a significant limitation in the form of a noticeable scarcity of empirical studies specifically focusing on this phenomenon within the South African context. Due to the limited availability of relevant literature, the researcher was unable to gather sufficient data to support a robust analysis. Furthermore, the scope of the literature review was deliberately confined to South African sources. While ensuring contextual relevance, this scope-induced limitation also resulted in the exclusion of potentially valuable international perspectives. This geographic restriction further narrowed the pool of eligible studies, thereby constraining the breadth and depth of the findings. Despite these limitations, the desktop approach provided a robust foundation for evaluating the role of SAPS in cybercrime enforcement and identification of strategic areas for improvement.

Data was collected through systematic searches in academic databases (e.g., Google Scholar, JSTOR), government websites (e.g., SAPS, Department of Justice), and reputable news outlets. Thematic analysis enabled the identification of patterns, gaps, and areas of progress in SAPS's cybercrime enforcement efforts (Modise, 2025). Keywords such as "cybercrime South Africa," "SAPS enforcement," "Cybercrimes Act," and "digital policing" were used to identify relevant materials published between 2019 and 2025. The collected data was analysed thematically, with key themes focusing on:

- Institutional capacity and skills gaps within the SAPS.
- Implementation and enforcement of the Cybercrimes Act, No. 19 of 2020.
- Public-private collaboration and international cooperation.
- Technological and procedural innovations in cybercrime investigation.

Findings and discussion

This study examined the role of the South African Police Service in enforcing the Cybercrimes Act No. 19 of 2020, focusing on its effectiveness and the challenges experienced in its implementation. The findings derived from the desktop review of academic literature, government reports, and legal analyses, reveal a complex landscape of progress and persistent obstacles. The SAPS's capacity to combat cybercrime is significantly affected by the limited cybercrime investigative expertise within specialised units, which are already burdened by the increasing cyber elements in traditional crime investigations (Aphane & Mofokeng, 2021). Cybercriminals are constantly developing new methods and techniques, requiring law enforcement to be agile and proactive in their response. This includes investing in new technologies, such as artificial intelligence and machine learning, which can enhance the ability to detect and prevent cybercrime. Cybercriminals use advanced tools such as malware attacks, phishing software and encryption to hide their actions, which compounds the efforts of law enforcement officials to keep abreast of these technologies (Matsaung & Masiloane, 2024). The high volume of sensitive personal and financial data generated by smart devices and platforms increases the risk of data breaches, identity theft, and financial fraud. These developments underscore the urgent need for South Africa to strengthen its cybercrime enforcement mechanisms, invest in digital skills development, and enhance collaboration with international partners to keep pace with the evolving threat landscape. Individuals, banks, and certain government departments have been targeted by illegal activities carried out through online systems. Unlike traditional crime, the borderless nature of cybercrime presents numerous challenges for international law enforcement agencies to address this form of crime through measures such as tracing perpetrators and enforcing the law across national borders. The global and anonymous nature of the internet allows cybercriminals to operate from anywhere around the world, often targeting victims in different countries. This borderless aspect complicates investigations, slackens international cooperation, and creates legal and jurisdictional hurdles that render the prevention and resolution of cybercrimes rather difficult (Ndubuisi, 2022).

Skills deficit and training gaps

The shortage of specialised skills within the SAPS constitutes a critical challenge. Cybercrime investigations require advanced technical competencies in digital forensics, encryption, and network analysis. Many officers currently lack these skills, which is exacerbated by the rapid evolution of cyber threats and potential to outpace the training and adaptation capacity of law enforcement (Schiliro, 2024). Cybercrime in African regions demands advanced skills and knowledge that surpass the capabilities of the average computer user, underscoring the need for specialised training and expertise in law enforcement (Mphatheni & Maluleke, 2022). Another critical area of concern relates to the training programmes for SAPS officers. While there have been efforts to provide cybercrime training, these programmes are often insufficient in scope and depth. Many officers receive only basic training, which does not equip them with the necessary skills to handle complex cybercrime cases (Amoo et. al., 2024). There is a compelling need for more comprehensive and continuous training programmes that cover the latest developments in cybercrime and cybersecurity. The research underscores the importance of continuous adaptation and innovation in law enforcement practices to keep pace with the dynamic nature of cybercrime. However, the effectiveness of these strategies is limited by several factors, including the lack of inter-agency collaboration. Cybercrime often involves multiple jurisdictions and requires cooperation between different domestic and international law enforcement agencies. The SAPS has struggled to establish effective partnerships with other agencies, which hinders this organisation's ability to confront cybercrime comprehensively.

Resource limitations and technological challenges

There are significant obstacles induced by the lack of adequate resources and specialised training within the South African Police Service, which impede the effective investigation and prosecution of cybercrimes (Fick, 2009). Despite the increasing prevalence of cybercrime, many SAPS officers are still trained primarily in traditional, analog-era policing methods, which are ill-suited for the complexities of digital investigations (Ige, 2020). This mismatch of skills severely limits the ability of law enforcement to respond to cyber threats in a timely and effective manner. The sophistication of cybercriminals further exacerbates this challenge. These actors often employ advanced technologies such as encryption, anonymisation tools, and artificial intelligence to evade detection. Moreover, they frequently operate across international borders, exploiting jurisdictional gaps and legislative inconsistencies between countries. Matsaung and Masiloane (2024) have noted that cybercrime transcends physical boundaries, allowing perpetrators to launch attacks from virtually anywhere in the world. This global nature of cybercrime complicates jurisdictional investigations, as SAPS must often rely on international cooperation and mutual legal assistance treaties (MLATs) in order to access evidence or apprehend suspects located abroad. Additionally, the lack of dedicated cybercrime infrastructure — such as digital forensic labs, real-time threat intelligence systems, and secure data-sharing platforms — further hampers the SAPS's operational capacity. Investigations are often delayed or compromised without these tools, which reduces the likelihood of successful prosecutions. The situation is compounded by limited budget allocations for cybercrime units, which struggle to retain skilled personnel due to better opportunities available in the private sector. It is imperative to develop and implement a multi-pronged strategy that includes continuous professional development, investment in digital infrastructure, and stronger partnerships with both domestic and international stakeholders in order to address these issues. It is only through such coordinated efforts that the SAPS could keep pace with the rapidly evolving threats in the cyber landscape.

Cybercrime units frequently operate under significant financial and operational constraints, which severely limit their capacity to conduct effective digital forensic investigations. Budget limitations often prevent these units from acquiring the advanced tools and technologies necessary for thorough analysis, such as specialised software for data recovery, malware analysis, and encrypted data access. Many of the law enforcement units operate with outdated equipment and lack proper software, making it difficult to handle digital evidence effectively and keeping pace with the rapidly evolving nature of cyber threats. These technological shortcomings hinder the proper collection, analysis, and preservation of digital evidence, which is critical for successful prosecution. Furthermore, cybercrime investigations are inherently complex and time-consuming, often requiring meticulous attention to detail and long hours of work. This places additional pressure on already limited personnel, many of whom may not have specialised training in digital forensics. The combination of limited resources, outdated infrastructure, and high labour demands significantly undermines the effectiveness of cybercrime units and highlights the urgent need for increased investment, capacity building, and international support (Shami, Saleem & Ashraf, 2025).

Collaboration and international engagement

South Africa has made progress in establishing legal and institutional frameworks to combat cybercrime, including the enactment of the Cybercrimes Act No. 19 of 2020 and participation in international agreements. However, these

tools alone are not sufficient. There are already mechanisms in place that provide a foundation for addressing cyber threats — such as legislation, bilateral and multilateral agreements, private sector initiatives, and platforms for information exchange. However, unilateral action remains inadequate in the face of increasingly sophisticated and transnational cybercrime networks. The borderlessness and complexity of the phenomenon of cybercrime demands a collaborative, multi-stakeholder approach. Accordingly, the public and private sectors should work in tandem in developing and implementing effective cybersecurity strategies. These include sharing of threat intelligence, coordinating incident response efforts, and jointly investing in cybersecurity infrastructure and training (Radanliev, 2024) Such collaboration ensures that both sectors benefit from each other's strengths — with government agencies bringing legal authority and enforcement capabilities, and private entities bringing advanced technical expertise and real-time threat detection systems. South African residents and institutions have increasingly become targets of cross-border cybercrime syndicates, which have attacked individuals, businesses, critical infrastructure, and even government systems. These attacks result in financial losses, and also threaten national security and public trust in digital systems. As such, proactive and coordinated responses are essential. These include the development of early warning systems, public awareness campaigns, and the integration of cybersecurity into national development strategies. Ultimately, addressing cybercrime effectively requires a whole-of-society approach, in terms of which law enforcement, the judiciary, private companies, academia, and civil society collaborate to build a resilient digital ecosystem. Failure to actualise such cooperation efforts in combating cybercrime will remain fragmented and reactive, leaving South Africa vulnerable to increasingly complex and damaging cyber threats.

Conclusion

Although South Africa has enacted the Cybercrimes Act to address the growing threat of cyber-related offences, the effective combating of cybercrime still remains a persistent challenge. Such a problematic state of affairs is induced primarily by the dynamic and constantly evolving nature of cyber threats, which often outpace the capacity of existing legal and enforcement frameworks. Law enforcement agencies and regulatory bodies are frequently left playing catch-up due to cybercriminals' continued development of more sophisticated methods of attack, which range from phishing and ransomware to identity theft and financial fraud. Coupled with jurisdictional complexities and limited local expertise in cyber forensics, the rapid advancement of digital technologies further complicates efforts towards the effective implementation of the Cybercrimes Act. Consequently, while the legislation provides a critical foundation, it is essential to ensure South Africa's continued resilience in the face of emerging cyber threats through measures such as ongoing adaptation, capacity-building, and international cooperation. The cybersecurity skills gap is a significant barrier to SAPS members, hindering their ability to effectively enforce the law. Additionally, the SAPS and other organisations lack the necessary capabilities to assess and monitor cyber threats on a daily basis, which is essential for protecting the nation's digital infrastructure and its citizens.

The effectiveness of the SAPS in combating cybercrime, particularly in investigations, should be thoroughly evaluated, as the Cybercrimes Act relies heavily on capable enforcement authorities. Furthermore, the SAPS should engage in international collaborations and global initiatives to combat cybercrime. This includes sharing information and best practices with other countries, as well as participating in joint operations to apprehend cybercriminals. It is imperative for South Africa to strengthens its enforcement mechanisms and invest in digital skills development, public awareness campaigns, and modernisation of its investigative infrastructure. Without such measures, the country risks falling further behind in the global fight against cybercrime in the 5IR era. Law enforcement personnel should receive training and resources to effectively combat cybercrime. Collaboration and partnerships with other countries in the fight against cybercrime are essential. This approach will benefit South Africa and allow us to learn from other nations, while demonstrating our willingness to participate actively in the battle against this global issue. There is also the challenge of training programmes that are often limited in scope and depth, with officers typically receiving only basic instruction — which is insufficient for handling complex cybercrime cases. There is a compelling demand for continuous professional development and specialised certifications for the purpose of ensuring that SAPS personnel remain current with global cybercrime trends.

Raising awareness about cyber hygiene and the importance of preserving digital evidence is crucial for preventing cybercrime and enabling early detection. Public education initiatives and tailored industry guidelines can empower individuals and organisations to recognise threats, reduce vulnerabilities, and report incidents promptly. The rapid and continuous technological evolutions have engendered both sophisticated cyber threats and innovative tools for investigation and evidence handling. Addressing these challenges requires a comprehensive approach that includes advanced training for forensic professionals, international collaboration to tackle cross-border crimes, strong public-private partnerships, and continuous innovation in digital forensic techniques. In addition, proactive adaption to the shifting digital landscape can enhance the effectiveness of cybercrime investigations by stakeholders, while also

ensuring the integrity of digital evidence, ultimately strengthening the legal response, and supporting the pursuit of justice.

Acknowledgements

This study was supported by the School of Criminal Justice, Department of Police Practice, College of Law at the University of South Africa.

Funding Statement: This study was not funded.

Disclosure of Interest: There are no conflicts of interest to declare.

Data Availability Statement: This study was conducted as a desktop-based literature review, systematically collecting and analysing secondary data from a wide range of credible sources

References

1. Adula, M., Kant, S., & Birbirsa, Z. A. (2023). Effects of training on organizational performance in the Ethiopian textile industry: Interview based investigation using MAXQDA. *IRASD Journal of Management, 5(1), 08-19.*
2. Amoo, O.O., Atadoga, A., Abrahams, T.O., Farayola, O.A., Osasona, F., & Ayinla, B.S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews, 21(2), 205-217.*
3. Apel, R. (2013). Sanctions, Perceptions, and Crime: Implications for Criminal Deterrence. J Quant Criminol 29, 67–101. https://doi.org/10.1007/s10940-012-9170-1
4. Aphane, M., & Mofokeng, J. (2021). South African Police Service capacity to respond to cybercrime: Challenges and potentials. *Journal of Southwest Jiaotong University, 56(4), 165-186.*
5. Aphane, M., & Mofokeng, T. (2020). Critical analysis of strategies towards creating an adequate level of awareness on cybercrime among the youth in Gauteng Province. *International Journal of Criminology and Sociology, 9.*
6. Atuguba, R. A. (2021). Legal pluralism in Africa: Three levels and seven types of law. In The Routledge Handbook of African Law (pp. 17-52). Routledge.
7. Bassot, B. (2022). Doing qualitative desk-based research: A practical guide to writing an excellent dissertation. Bristol: Bristol University Press.
8. Bote, M. (2019). Cybercrime legislation in South Africa: An analysis of the Cybercrimes Bill. *South African Yearbook of International Law*, 44, 89–104.
9. Clarke, R. (2018). The Theory and Practice of Situational Crime Prevention. Oxford Research Encyclopedia of Criminology. https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-327.
10. Cybersecurity Hub. (2025). Cybercrime incidents and national response 2023–2025. South African Department of Communications and Digital Technologies. Available at: https://www.cybersecurityhub.gov.za
11. de Melo, S. N., Pereira, D. V. S., Andresen, M. A., & Matias, L. F. (2017). Spatial/Temporal Variations of Crime: A Routine Activity Theory Perspective. International Journal of Offender Therapy and Comparative Criminology, 62(7), 1967-1991. https://doi.org/10.1177/0306624X17703654
12. Du Toit, P. (2024). Legal challenges in enforcing the Cybercrimes Act: A procedural analysis. *University of Pretoria Law Revie*w, 31(2), 45–62.
13. Ezeji, C. L. (2024). Cyber policy for monitoring and regulating cyberspace and cyber security measures for combating technologically enhanced crime in South Africa. *International Journal of Business Ecosystem & Strategy, 6(5), 96–109. https://doi.org/10.36096/ijbes.v6i5.670*
14. Fick, J. (2009). Challenges in policing cybercrime in South Africa. *South African Journal of Criminal Justice, 22(1), 56–72.*
15. Fink, A. (2019). Conducting research literature reviews: From the internet to paper. Thousand Oaks, CA: Sage Publications.
16. Henrico, S., & Els, S. (2025). Cyber attacks in South Africa: Geopolitical and legal implications. *African Security Review, 1–25. https://doi.org/10.1080/10246029.2025.2489352*

17. Govender, S. (2024). Cybercrime enforcement in South Africa: Capacity, training, and collaboration. *South African Journal of Criminal Justice, 37(1), 88–105.*
18. Ige, O. (2020). Digital policing in Africa: Bridging the skills gap in law enforcement. *African Journal of Cybersecurity, 5(2), 101–117.*
19. Institute for Digital Security and Innovation. (IDSI). (2024). Cybersecurity readiness in South Africa: A national review. Pretoria: IDSI Publications.
20. INTERPOL. (2024). African Cyberthreat Assessment Report 2024 (3rd ed.). African cybercrime operations desk. Available at: https://afripol.africa-union.org/uploads/files/24com005030-ajfoc_africa-cyberthreat-assessment-report_2024_complet_en-v4.pdf
21. IRMSA. (2024). IRMSA Risk Report 2024: South Africa's Risk Landscape. Institute of Risk Management South Africa. Available at: https://www.irmsa.org.za
22. Matsaung, P., & Masiloane, D. T. (2024). The role of cyber intelligence in policing cybercrime in South Africa: Insights from law enforcement officers. *African Security Review, 34(2), 152–167. https://doi.org/10.1080/10246029.2024.2421225*
23. Mohammed, S., Dlamini, Z., & Modise, M. (2019). Situational crime prevention in cyberspace: A South African case study. *South African Journal of Criminal Justice, 32(2), 210–229*.
24. Mpahlwa, M. (2025). How can South Africa combat the growing threat of cybercrime? De Rebus. Available at https://www.derebus.org.za/category/columns/feature-articles/
25. Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science (2147- 4478), 11(4), 384–396. https://doi.org/10.20525/ijrbs.v11i4.1714*
26. Ndubuisi, A. F. (2022). Cross-border jurisdiction challenges in prosecuting cybercrime syndicates targeting national financial and electoral systems. *International Journal of Engineering Technology Research & Management, 6(11).*
27. Nelufule, N., Masango, M., & Singano, T. (2024). Digital forensics in industry 4.0 and industry 5.0: Major challenges and opportunities. *In 2024 47th MIPRO ICT and Electronics Convention (MIPRO) (pp. 1849-1854). IEEE.*
28. Pieterse, H. (2021). Cybersecurity capacity and law enforcement readiness in South Africa. *South African Journal of Criminal Justice, 34(2), 145–162.* https://doi.org/10.10520/EJC-2021-34-2
29. Press Council of South Africa. (2024). Cybercrime and digital safety: The role of media and regulation. Available at: https://www.presscouncil.org.za/reports/cybercrime-2024
30. Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, blockchains, and Quantum Computing. *Journal of Cyber Security Technology, 9(1), 28-78.*
31. Rao, Y. S., & Pradhan, D. (2020). Digital crime and its impact in present society. *International Journal of Engineering Research & Technology, 8(1). https://doi.org/10.1080/23742917.2024.2312671*
32. Riffe, D., Lacy, S., Watson, B. R., & Lovejoy, J. (2023). Analyzing media messages: Using quantitative content analysis in research. New York*:* Routledge.
33. Schiliro, F. (2024). From Crime to Hypercrime: Evolving Threats and Law Enforcement's New Mandate in the AI Age. arXiv preprint arXiv:2411.10995.
34. Shami, A. Z. A., Saleem, M., & Ashraf, J. (2025). Cybercrime and digital evidence: investigating the challenges and opportunities in prosecuting cybercrime and handling digital evidence. *Research Consortium Archive, 3(2), 400-411.*
35. Shingange, T. (2024). Policy fragmentation and the implementation of South Africa's national cybersecurity policy framework. *South African Journal of Public Administration, 59(1), 45–62.*
36. Singh, R. (2024). AI-driven cybercrime and the rise of MalFE: A new frontier in digital threats. *Journal of Cybersecurity Innovation, 6(1), 45–59.*
37. Press Council of South Africa. (2024, November 4). Cybercrimes Act: What you need to know. Available at: https://presscouncil.org.za/2024/11/04/cybercrimes-act-what-you-need-to-know/
38. Snail ka Mtuze, 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. Available at: *Obiter*, 43(3). https://scielo.org.za/scielo.php?script=sci_arttext&pid=S1682-58532022000300006

39. Sophos. (2024, April 30). The state of ransomware 2024. Available at: https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/
40. South Africa. (2020). Cybercrimes Act 19 of 2020. Government Gazette, 664(43716). Pretoria: Government Printers.
41. South African Police Service. (2023). Standard Operating Procedures in Terms of Section 26 of the Cybercrimes Act, No. 19 of 2020. Available at: https://www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf
42. South African Police Service. (2022). Draft Standard Operating Procedures for the Investigation, Search, Access or Seizure of Electronic Evidence in terms of Section 26 of the Cybercrimes Act, No. 19 of 2020. Available at: https://www.lssa.org.za/wp-content/uploads/2022/05/Draft-SAPS-CCA-SOP-20220509-V7-JF-003.pdf
43. South African Police Service. (2022). SAPS Legal and Policy Framework: Protection Service. Available at: https://pmg.org.za/files/220128_SAPS_presentation.pdf
44. The Press Council of South Africa. (2024, November 4). Cybercrimes Act: What you need to know. Available at: https://presscouncil.org.za/2024/11/04/cybercrimes-act-what-you-need-to-know/
45. University of Cape Town. (2024). Standard operating procedures (SOP) in terms of the Cybercrimes Act. UCT Law@work. Available at: https://law.uct.ac.za/law-at-work/courses/sop-cybercrime-act
46. Van Niekerk, B., & Maharaj, M. (2022). Cybersecurity awareness and routine activity theory: A South African perspective. *Journal of Information Warfare, 21(3), 45-60.*
47. Wendt, D.W. (2024). Combatting Generative AI Threats. In: The Cybersecurity Trinity. Apress, Berkeley, CA. https://doi.org/10.1007/979-8-8688-0947-7_5
48. Ziatdinov, R., Atteraya, M. S., & Nabiyev, R. (2024). The fifth industrial revolution as a transformative step towards society 5.0. *Societies, 14(2), 19*. https://doi.org/10.3390/soc14020019