Article

Digital Disruption and the Transformation of Private Security Services in South Africa: An Examination of Emerging Technologies

Tladi Paul Maja
https://orcid.org/0009-0007-5514-1694
University of South Africa
majatp@unisa.ac.za

Kris Pillay
https://orcid.org/0000-0001-8599-4099
University of South Africa
cpillay@unisa.ac.za

Abstract

South Africa's private security industry is experiencing a profound transformation driven by digital disruption and the implementation of emerging technologies. Using documentary analysis, this article examines how innovations such as artificial intelligence (AI), drones, Internet of Things (IoT) sensors, biometric authentication, and cybersecurity systems are transforming the delivery of security services. Although these technologies enable predictive analytics, real-time threat detection, and automated incident response, they also present complex challenges related to privacy, regulation, and skills and workforce deficits. This article draws on socio-technical systems theory and surveillance studies. The study examines the crossroads of technological adoption with governance, regulations, ethics, and social equity. It also employs qualitative content analysis of academic literature, government reports, and industry publications to identify key trends, benefits, and limitations. This approach helps achieve the aim by demonstrating how AI and related technologies impact security service delivery, while also identifying the regulatory, ethical, and skills factors that influence their effective use. The findings reveal significant gaps in regulatory frameworks, particularly the outdated provisions of the Private Security Industry Regulation Act 56 of 2002 (PSIRA Act 56 of 2002) and highlight the need for inclusive training programmes to address digital competency deficits among security personnel. The recommendations include legal reform and more empirical studies on the effectiveness of upskilling workforce development. This research contributes to a deeper understanding of the evolving role and use of digital technologies among security service providers in South Africa and provides policy-relevant insights for ensuring the ethical and equitable integration and regulation of digital technologies within the sector.

Keywords: private security industry; digital disruption; emerging technologies;

UNISA university of south africa PRESS
Southern African Journal of Security
#20848| 18 pages

https://doi.org/10.25159/3005-4222/20848
ISSN 3005-4222 (Online),

Artificial Intelligence (AI); Internet of Things (IoT); biometric surveillance

Introduction

South Africa's private security industry has emerged as one of the largest and most significant sectors globally, representing a critical component of the nation's security landscape (Berg 2020). The sector plays a critical role in supplementing public law enforcement, particularly in contexts where state capacity is limited or overstretched (Gumedze 2015). It contributes not only to national safety and crime prevention but also to employment creation and economic activity, making it a vital component of South Africa's broader security and socio-economic landscape (Button 2025). Traditional private security in South Africa historically relied on static guarding, basic alarm systems, and manual patrol routes (Gumedze 2015). Today, the industry's digital transformation has introduced state-of-the-art technologies, including artificial intelligence-powered surveillance systems, Internet of Things (IoT) sensors, biometric access controls, drone surveillance, predictive analytics, and integrated command and control centres (Caluza 2022). These technologies are not merely supplementing existing services but are fundamentally redefining future security service delivery models.

Digital disruption has enabled private security companies to offer predictive security analytics, real-time threat assessment, automated incident response, remote monitoring capabilities, and data-driven security consulting (Caluza 2022). Despite this rapid evolution, a significant gap remains in the academic literature regarding the critical examination of how these technologies are being adopted, implemented, and governed within the South African private security sector. This paper aims to address that gap by evaluating the transformative impact of digital disruption on private security services in South Africa. It examines the opportunities and challenges presented by emerging technologies, with a specific focus on operational effectiveness, ethical implications, regulatory frameworks, and social equity.

Literature Review

Private Security Industry in South Africa

The scale of the private security industry becomes particularly evident when examining employment figures. The industry comprises more than 14,000 registered companies, establishing it as a substantial economic force within the country's service sector (PSIRA Annual Report 2024). More than 2.7 million private security officers are registered in the country, making the security industry one of the largest in the world (PSIRA Annual Report 2024). However, it is essential to distinguish between registered and actively employed personnel, as the number of security officers actively employed across the country is significantly lower (564,540), according to the PSIRA data (PSIRA Annual Report 2024). The industry's financial magnitude is equally impressive, with growth estimated to reach a value of R50 billion (Berg 2020). PSIRA operates with a

budget of R452.7 million in 2023/24, representing a nominal increase of 10.5 per cent, with projected expenditure growth to R605 million in 2026/27 (PSIRA Annual Report 2024). When compared to South Africa's state security apparatus, the private security sector significantly outnumbers the State Security Forces. SAPS' latest annual report indicates a fixed establishment of 182,126 employees, whereas studies have shown that South Africa has 2.57 private security personnel for every police employee (PSIRA Annual Report 2024). This ratio demonstrates the substantial reliance on private security services to supplement state security capabilities.

In South Africa, a nation characterised by high crime rates and a complex security landscape, private security companies have increasingly integrated advanced technological solutions to address these challenges (Caluza 2022). However, the strategy fails to comprehensively examine how technological transformation affects individual security practitioners whose professional roles are being fundamentally altered by automation and digital innovation. Research in South Africa has focused more on crime prevention and less on how security technologies can be deployed to enhance crime prevention initiatives and their impact. For example, Magliocca et. al. (2025) emphasise the convergence of safety and security in modern systems, noting the increasing complexity of managing human-technology interactions (Phillips 2022).

These technologies include physical systems (such as access control, CCTV, and biometrics), cybersecurity solutions, and advanced surveillance technologies, including drones, facial recognition, and response capabilities. It is worth noting that the adoption of modern technologies has become a critical driver of quality service provision among security companies in their efforts to combat crime (Ekwenye, Theuri, and Mwenda 2018). The digital transformation of South Africa's security industry represents a shift from traditional labour-based services to technology-enabled solutions that address security challenges with greater sophistication. This literature review critically examines some of the most prominent emerging technologies, including Artificial Intelligence (AI), drones, the Internet of Things (IoT), biometric authentication, and cybersecurity measures, and explores their adoption and impact within the South African private security sector.

Artificial Intelligence and Machine Learning

AI and Machine Learning (ML) have become central to modern security systems by enabling predictive analytics and automating surveillance processes. These technologies study vast data streams to identify suspicious behaviour, recognise faces, and detect anomalies in real-time (Fahad, Anwar, and Nawaz 2022). In response to elevated crime rates in major urban centres, private security companies in South Africa have progressively implemented AI-driven surveillance systems, with notable deployments in Johannesburg and Cape Town (Masombuka 2018). For instance, AI-powered CCTV systems are used to automatically flag unusual activities, reducing the need for manual monitoring and enabling quicker response times (Fahad et al. 2022). AI-powered

surveillance systems can automatically detect unusual activities or unauthorised access, reducing the need for human monitoring and increasing response efficiency (Van Steenen and De Waard 2023). AI-powered surveillance represents a significant technological advancement in the sector. The Vumacam Project in the City of Johannesburg surveillance network exemplifies this trend by using facial recognition technology and automated threat detection systems. The company operates a subscription-based model, allowing private security companies and law enforcement agencies to access clustered camera feeds through the Proof 360 platform (Bulbulia 2024). Critical developments include the implementation of facial recognition systems across urban surveillance networks, integration with the proposed national biometric identification database (ABIS), and the use of automated license plate recognition systems, as well as AI-powered behavioural analysis and threat detection algorithms. Thus, AI-driven systems can also automate routine tasks, such as monitoring multiple camera feeds simultaneously, freeing human operators for more complex decision-making. These technologies are particularly useful in high-traffic areas or large facilities where manual monitoring is impractical (Kumar 2023).

Drones and Unmanned Aerial Vehicles (UAVs)

The literature of the most prominent emerging technologies reveals extensive adoption of drone technology across multiple private security applications in South Africa (Nkhoma and Agbenyegah 2021). UAVs are being deployed for perimeter security, crowd monitoring, and rapid response scenarios. Drones have revolutionised perimeter security and surveillance, especially in large or inaccessible terrains. Equipped with high-definition and thermal imaging cameras, drones provide aerial views that enhance situational awareness (Smith and Lee 2023). The technology provides "increased visibility, real-time views, faster travel times, and the benefit that it is often undetected" (Drone 2021). Key developments include the integration of thermal and night vision cameras for enhanced surveillance capabilities and autonomous flight operations, which reduce the need for on-site pilots. In addition, centralised command and control systems enable wider coverage with fewer personnel (Fahad 2022).

Drones have been deployed in specialised applications in mining security, anti-poaching, and critical infrastructure protection (Smith and Lee 2023). In South Africa, private security companies such as Securitas and G4S have used drones for perimeter patrols of critical infrastructure, including mines, power stations, and large commercial properties. For example, during the 2022 mining sector disruptions, drones were deployed to monitor vast mine perimeters, providing real-time intelligence on unauthorised intrusions and reducing the need for manual patrols in risky environments (Smith and Lee 2023). Some private security firms use autonomous drones that operate on pre-programmed routes or respond to specific triggers, such as motion detection. The integration of AI enables drones to autonomously identify potential threats, alerting human operators to take further action (Smith and Lee 2023).

Internet of Things (IoT) Sensors

IoT sensors enable integrated, continuous monitoring through interconnected devices, including smart alarms, environmental sensors, fire detection and access controls (Kumar et al. 2023). South African security firms have integrated IoT into their offerings, particularly in high-security facilities like data centres, casinos, and government buildings. For example, a prominent security service provider has implemented IoT-enabled environmental sensors in Johannesburg-based data centres to detect smoke, gas leaks, and temperature fluctuations, triggering automated responses and alerts that prevent security breaches and operational disruptions (Ngwenya and Ngoepe 2020). IoT sensors are particularly valuable in sensitive environments, such as data centres, warehouses, or high-security facilities, where continuous, real-time monitoring is critical. They also facilitate predictive maintenance, alerting staff to equipment malfunctions before they cause security breaches or operational disruptions (Kumar et al. 2023).

Biometric Authentication Technologies

Biometric technology has seen substantial growth in the private security sector, with the global biometric access control market projected to reach significant valuations (Rahman and Patel 2022). Biometric authentication enhances security by eliminating vulnerabilities associated with traditional password or ID card systems, which can be lost, stolen, or shared. Key applications of biometric technologies include fingerprint and facial recognition, as well as access control and multi-modal biometric systems that combine multiple authentication methods. It also streamlines entry processes, reducing wait times and enhancing user convenience, particularly in high-security environments such as corporate offices, airports, or government facilities (Rahman and Patel 2022). These contactless and highly accurate systems are increasingly adopted in South Africa's high-security environments, such as airports, government facilities, and corporate offices (Dagada 2024). For instance, South African Airports Company (ACSA) has integrated biometric facial recognition at several international airports to streamline passenger verification and enhance border security, aligning with global trends in biometric authentication (Dagada 2024).

Cybersecurity Measures

As private security increasingly relies on interconnected digital systems, protecting these networks from cyber threats has become paramount (Warfield 2012). South African security companies use advanced cybersecurity tools, including intrusion detection systems, encryption, and threat intelligence platforms, to safeguard against cyberattacks that could compromise physical security systems (Williams and Chen 2023). For example, G4S South Africa has invested in cybersecurity infrastructure to safeguard its integrated security systems across multiple sites, ensuring resilience

against cyber threats and maintaining operational integrity (G4S Risk Management n.d.).

Modern private security companies leverage AI and ML for predictive analytics, drones for aerial surveillance, IoT sensors for real-time monitoring, biometric authentication for access control, and cybersecurity measures to safeguard digital assets (Michael 2025). These technologies collectively enhance the effectiveness, efficiency, and safety of private security operations. The adoption of these emerging technologies reflects a significant shift in South Africa's private security landscape, driven by the need for more effective, efficient, and proactive security solutions. While these systems offer operational efficiencies and faster emergency response, they deepen concerns regarding privacy, ethical accountability, and technological dependence. The convergence of multiple surveillance technologies into single platforms significantly increases data collection capabilities, yet regulatory frameworks have not kept pace with these developments (Vermesan and Friess 2013). Industry discussions often prioritise the security advantages of digital technologies, giving less attention to questions of proportionality, necessity, and potential surveillance expansion. As private security firms continue to adopt digital systems, the limited development of formal ethical guidelines in South Africa may raise considerations for civil liberties and mechanisms of public accountability.

Therefore, a critical evaluation of these technologies must extend beyond operational efficiency to examine their broader societal implications and potential for misuse.

Human Impact and Labour Implications

The integration of digital technologies into private security operations has a significant impact on employment patterns and job roles, and AI-driven systems are displacing traditional roles, which requires the retraining and upskilling of security technicians. Studies indicate that job insecurity is increasing among security officers due to technological advancements (Nam 2019). Ahmed, Qin and Martínez (2019) highlight the psychological impact of technological anxiety and the need for proactive workforce development strategies. In another study, it was confirmed that there is a growing demand for digital literacy, cybersecurity awareness, and technical proficiency in operating surveillance and biometric systems (Chibunna, Hamza, Collins, Onoja, Eweja, and Daraojimba 2020). It is imperative that training programmes be systematically aligned with the evolving technological competencies required in the sector. Therefore, it is imperative that training programmes are aligned with emerging technological trends to ensure a sustainable transition for the security workforce.

Regulatory Framework Analysis

Although the PSIRA Act 56 of 2001 has been in operation for almost 25 years, South Africa's regulatory framework for private security technologies lags behind

international standards. While the Private Security Industry Regulation Act (PSIRA 2001) provides general oversight of the sector, it contains no specific provisions governing AI systems, biometric technologies, or drone surveillance (Minnaar 2018). By comparison, the European Union has established comprehensive regulatory mechanisms through the General Data Protection Regulation (GDPR) (European Parliament and Council 2016) and the proposed AI Act (European Commission 2021), which address data protection and algorithmic accountability, respectively. The Institute for Security Studies (2023) advocates for human-centric AI regulation within the South African context. To address these regulatory gaps, PSIRA requires substantive amendments incorporating ethical guidelines, transparency requirements, and compliance mechanisms tailored to emerging technologies (Berg and Nouveau 2021).

Conceptual Framework

This study adopts a critical lens informed by socio-technical systems theory developed by Eric Trist and Ken Bamforth in the 1950s. The socio-technical systems theory posits that technology and social systems are not separate entities, but rather interdependent, necessitating a more comprehensive analysis of their relationships (Trist and Bamforth 1951). However, this framework has been critiqued for its tendency towards technological determinism and its repeated co-option by management decisions that prioritise efficiency over equity (Bridges, Moyo, and Sibanda 2018). In the context of private security, socio-technical analysis must not only examine how technology and human actors interact, but also consider whose interests these interactions serve, and which populations bear disproportionate costs.

Surveillance studies, on the other hand, help to explain how AI and biometrics are used to categorise populations, maintain power inequalities, and exercise control (Lyon 2008). Security technologies serve as tools for data collection and profiling, changing the relationship between security providers and citizens (Lyon 2008). Biometric systems contain racial and gender biases that disproportionately harm marginalised communities (Lyon 2008), while AI surveillance has normalised constant monitoring in urban environments (Aale 2023). The privatisation of surveillance technologies raises concerns about accountability, as private security firms operate with less oversight than government agencies, despite possessing similar technological capabilities (Dickson 2011).

These frameworks demonstrate that technological adoption in private security is not neutral, but rather represents a contested space where commercial interests, state power, and civil liberties intersect. Emerging technologies must therefore be evaluated beyond operational efficiency to examine how they reinforce social inequalities, expand surveillance infrastructure, and undermine democratic accountability (Fussey and Murray 2019).

Methodology

This study aims to critically examine the impact of digital disruption on the private security sector in South Africa by examining how emerging technologies, such as AI, drones, the Internet of Things, biometric authentication, and cybersecurity measures, are transforming security practices and service delivery. A qualitative research design employing thematic content analysis as the primary method for analysing textual data was employed. Qualitative research is particularly well-suited to this inquiry because it enables the interpretation of complex social phenomena through rich, descriptive data. It was chosen to facilitate an in-depth understanding of how emerging technologies are transforming private security services in South Africa. A purposive selection of literature published between 2015 and 2025 was undertaken. Data sources included peer-reviewed academic publications, South African government reports, and industry documents accessed through scholarly databases, policy repositories, and professional platforms. Sources were included if they addressed emerging or digital security technologies and demonstrated empirical, regulatory, or conceptual relevance to the South African private security industry. Materials lacking analytical depth or contextual relevance were excluded. The final corpus was systematically analysed to identify key themes related to technological adoption, with particular attention to governance, regulatory frameworks, ethical considerations, and workforce implications. This process revealed how these technologies are shaping private security practices in South Africa, including both their practical deployment and the broader context of their use.

Data Analysis

This study employed thematic analysis to systematically identify and interpret patterns within the textual data (Braun and Clarke 2022). The analysis followed an iterative process comprising five key stages. First, the researchers familiarised themselves with the collected materials—academic articles, government reports, industry publications, and deployment plans—through repeated reading to gain a comprehensive understanding of technological adoption in the sector. Second, initial codes were generated by systematically annotating text segments related to technological applications, benefits, challenges, and ethical considerations. Third, coded data were examined to identify patterns, with related codes grouped into broader thematic categories. For example, references to AI threat detection, drone surveillance, and IoT monitoring were consolidated under the theme “Technological Applications in Security.” Fourth, themes underwent iterative review and refinement to ensure they accurately represented the data and maintained distinctiveness. Finally, themes were interpreted within the research context, revealing critical insights into the transformation of private security in South Africa. The following key themes emerged: Benefits of technology adoption, operational challenges, and literature gaps and research opportunities, which formed the foundation for subsequent analysis.

Discussion of Findings

This discussion interprets the study's findings through the frameworks of socio-technical systems (STS) and surveillance studies to explain how emerging technologies—AI, drones, Internet of Things (IoT) sensors, biometrics, and cybersecurity—transform private security service delivery in South Africa.

Theme 1 - Benefits of Technology Adoption

The most effective physical security technologies employed in the access control system include advanced biometric authentication scanners (fingerprint technologies), which provide a higher security level than traditional access card methods, integrated with electronic logs at the entry points (Mondela and Sirera 2023). Closed-circuit television (CCTV) systems are used for real-time monitoring of physical access control and recording footage for later analysis. They are often coupled with intelligent alarm sensors and electronic intruder alarm systems that detect unauthorised access and trigger a response protocol, thereby enhancing perimeter protection at all boundaries of the property. These technologies require security practitioners to be proficient in operating them (Mondela and Sirera 2023).

The implementation of these technologies is significantly reshaping the protective security industry in South Africa, thereby aligning itself with global trends in automation, digitisation, and smart/intelligent systems. Innovations such as AI, biometric access control, smart surveillance, and the Internet of Things (Iot) are increasingly integrated into private security operations (Caluza 2022). These technologies enhance real-time monitoring, predictive threat detection, and remote response capabilities, enabling security firms to deliver more efficient and scalable services (Phillips 2022).

While AI can enhance anomaly detection and response speed, the analysis reveals that performance improvements require the concurrent optimisation of workflows, role design, and data governance. From an STS perspective, AI deployment can alter the task boundaries and impact the decision-making cycles of control room operators. It can introduce new failure modes (false positives, alarm fatigue) and shadow practices where staff bypass systems to meet operational targets (Trist and Bamforth 1951; Emery and Trist 1960).

Increasingly, South African businesses rely on Virtual Private Networks (VPNs) to establish secure internet connections, especially important during remote work scenarios (Ncubukezi 2022). At the centre are advanced algorithms of AI and Machine Learning, which are used for intrusion detection, threat analysis, and behavioural analytics (Kumar et. al. 2010). With the rise of cyber threats, security practitioners are increasingly required to manage cybersecurity protocols, which include incident response and risk assessment (Solms 2023).

As private security companies transition to digital systems, their operations only work reliably if they are protected from cyberattacks. These systems link cameras, sensors, analytics software, and control rooms into one platform. The findings indicate that many companies, particularly smaller ones, lack the necessary skills, tools, and ongoing funding to effectively secure these systems, monitor them properly, and respond to incidents. Research confirms there is a worldwide shortage of cybersecurity expertise, which makes it harder for companies to set up and maintain secure systems (Furnell and Shah 2020).

Theme 2 - Operational Challenges

The analysis found that although AI enhances threat detection and predictive analytics, its deployment in security systems raises concerns about algorithm manipulation and transparency in decision-making. Malicious actors can exploit vulnerabilities in AI models, potentially leading to false alarms or compromised responses (Pear 2025). Drones are increasingly used for surveillance and emergency response, offering faster inspections and broader coverage. However, they face certain drawbacks, for example, cybersecurity risks such as unauthorised access, data interception, and navigation control weaknesses. These vulnerabilities can disrupt operations and compromise public safety (Brudner 2024; Pear 2025).

While cybersecurity frameworks are essential for protecting digital infrastructure, many security providers struggle with implementation due to limited resources and expertise. The complexity of securing AI-driven and IoT-enabled systems demands continuous updates, monitoring, and skilled personnel. According to the South African Police Service's 2025/2026 Annual Performance Plan, the integration of digital technologies into policing requires robust cybersecurity measures to safeguard sensitive systems and data.

Internet of Things (IoT) devices facilitate real-time monitoring and seamless data exchange across security networks, significantly enhancing operational efficiency. However, their interconnected architecture also introduces some security risks, making them prone to denial-of-service (DoS) attacks, data breaches, and unauthorised access (Nayak et al. 2025). Therefore, ensuring the security of communications and maintaining the integrity of these devices remains a critical operational challenge that demands continuous oversight and investment in secure infrastructure.

Biometric systems have significantly improved access control by offering more secure and user-specific identification methods. However, their implementation raises important privacy concerns and necessitates strong data protection measures. Operational challenges include the potential for false positives, system malfunctions, and the theft of biometric data, which are particularly serious given the permanent and unique nature of biometric identifiers. In South African deployments, the efficiency gains reported at airports and corporate facilities are tempered by privacy and consent requirements, including data minimisation, purpose limitation, and secure storage

aligned with POPIA and international norms such as the GDPR (Dagada 2024; European Parliament and Council 2016). Surveillance studies caution that normalising biometric checks can alter everyday relations between security providers and citizens, underscoring the need for transparent redress mechanisms (including contesting decisions and deletion requests) and public communication on retention and sharing (Lyon 2008; Sutherland and Jamieson 2021).

While AI can enhance threat detection and expedite responses in control rooms, these benefits depend on high-quality data, effective staff training, and optimised workflows. From a socio-technical systems perspective, introducing AI changes job roles and decision-making processes. Without careful alignment between technology, human responsibilities, and procedures, organisations may experience problems such as false alarms and operator fatigue. Surveillance studies also caution that expanding analytics, such as facial recognition and licence plate recognition, can lead to unintended uses, weak consent practices, and uneven oversight.

Theme 3: Literature Gaps and Research Opportunities

Regulatory and Legal Framework Analysis

The literature review revealed a significant lacuna in scholarly examination of South Africa's regulatory response to emerging security technologies. While the Private Security Industry Regulation Act (PSIRA 2001) provides foundational oversight of the industry, academic engagement with its adequacy for governing AI, biometrics, and autonomous systems remains superficial and fragmented (Berg and Nouveau 2021). This gap is particularly concerning given the rapid technological transformation occurring within the sector, which has substantially outpaced legislative adaptation (Berg and Nouveau 2021).

Another critique is that existing scholarship has failed to systematically assess whether PSIRA's current provisions, designed for a pre-digital security landscape, can effectively govern algorithmic decision-making, automated surveillance, and data-intensive security practices. The paucity of policy-oriented research is equally problematic. Academic literature has not generated substantive recommendations for legislative reform that balance security imperatives with civil liberties protections (Sutherland and Jamieson 2021).

Privacy Issues

There is a notable lack of empirical research on the privacy risks associated with privately operated surveillance systems in South Africa, particularly those using facial recognition and biometric data. This gap is concerning, given the rapid expansion of such technologies in the private security sector, which often operates with less transparency than public law enforcement. The absence of thorough privacy assessments highlights the need to critically examine how these technologies are reshaping the boundaries between public and private surveillance. Research has

insufficiently examined how biometric data collection by private security firms affects individuals' control over their bodies and personal information.

The examination reveals that South African private security companies are increasingly deploying facial recognition systems in residential estates, shopping centres, and transport hubs; however, scholarly examination of the privacy implications remains underdeveloped (Clarno 2013). Research has not adequately addressed several fundamental questions: What happens to biometric data after it is initially collected? How long is it retained? With whom is it shared? Under what circumstances can individuals request deletion? The secrecy surrounding these practices indicates that biometric surveillance is being accepted as normal in cities, rather than being questioned and debated publicly (Norris and Armstrong 1999).

Effectiveness and Performance Evaluation

The review reveals a significant empirical gap in evaluating whether emerging security technologies deliver their promised outcomes. Despite substantial industry investment in AI-driven surveillance, biometric systems, and autonomous monitoring technologies, rigorous quantitative assessment of their actual effectiveness in reducing crime or improving security remains conspicuously absent (Welsh and Farrington 2009). Scholarly literature has failed to establish causal relationships between the deployment of technology and crime reduction outcomes in South African private security contexts. While industry reports frequently claim enhanced detection capabilities and faster response times, these assertions rarely undergo independent verification or methodologically rigorous testing (Lab 2015). The opportunity is available to conduct longitudinal studies that measure the impact of security technology on crime prevention and detection rates.

Economic Impact Analysis

Despite the growing integration of advanced technologies in South Africa's private security sector, a significant gap remains in empirical research evaluating the economic implications of this transformation. The adoption of AI, drones, IoT systems, and biometric technologies involves substantial upfront investment, continuous maintenance costs, and workforce reskilling expenses. However, few studies have systematically assessed the return on investment (ROI) or the cost-benefit dynamics of these implementations. ROI analysis should consider both tangible outcomes (e.g., reduced theft, faster response times) and intangible benefits (e.g., enhanced client trust, brand reputation). Economic analysis must explain the impact on employment patterns, including job displacement, wage shifts, and the emergence of new roles requiring digital competencies (Ahmed 2019). These changes have broader implications for socioeconomic equity and workforce sustainability. This creates a research opportunity to conduct a cost-benefit analysis of different technology implementations and their impact on industry competitiveness.

Social Inequality and Digital Divide

The rapid adoption of advanced security technologies, such as AI surveillance, biometric access systems, and IoT-enabled monitoring, has introduced new layers of inequality within South Africa's socio-economic landscape (Gordon, Booysen, and Mbonigaba 2020). While these innovations enhance operational efficiency and threat detection, their deployment is often concentrated in affluent urban areas, gated communities, and corporate environments. This uneven distribution, especially in South Africa, raises concerns about differential access to security, where wealthier communities benefit from enhanced protection while lower-income areas remain underserved. Communities lacking digital infrastructure or technical literacy may be excluded from the benefits of smart security systems. This exclusion not only affects physical safety but also limits participation in broader digital ecosystems, contributing to social marginalisation (Gordon et al. 2020). The shift towards automation and AI may displace low-skilled security workers, many of whom come from disadvantaged backgrounds. Without targeted reskilling initiatives, this transition risks exacerbating unemployment and economic vulnerability. An opportunity exists to conduct studies on differential access to advanced security technologies, upskilling initiatives and their social implications.

Cybersecurity and System Vulnerabilities

As private security services increasingly rely on interconnected digital systems, there is a limited understanding of the cybersecurity risks associated with connected security systems and possible weaknesses in private security networks. A research opportunity exists to conduct security assessments of IoT-enabled security systems and develop cybersecurity best practices.

Training and Skills Development

The shift to digital technologies in South Africa's private security sector has created an urgent need for updated training and skills development. As tools such as AI, drones, IoT, and biometrics become increasingly central to operations, many security personnel lack the necessary skills. Without targeted reskilling initiatives, the shift towards automation risks excluding older or lower-skilled workers from the evolving job market. Inclusive training strategies are needed to ensure equitable participation and prevent technological unemployment. However, there is limited research on how the industry addresses this challenge through workforce training, certification, or institutional support. There is limited coordination between private firms, regulatory bodies (e.g., PSIRA), and educational institutions to develop responsive training frameworks. Policy interventions could incentivise upskilling and promote partnerships for curriculum development. A research opportunity exists to conduct an analysis of training programmes, certification requirements, and workforce development needs in the digitised security sector.

Conclusion

This literature review of digital disruption and the transformation of private security services in South Africa identifies several critical research gaps, including outdated regulatory frameworks, inadequate privacy protections, and the evaluation of their effectiveness, as well as the economic impact, influence on social inequality, cybersecurity, and skills and workforce development. Additionally, the Private Security Industry Regulation Act (PSIRA 2001) has not kept pace with technological advancements, lacking provisions for AI, biometrics, and autonomous systems. Privacy concerns are growing due to the lack of clear rules on how biometric data—especially from facial recognition systems—is stored, shared, or deleted, as these technologies expand into residential areas and shopping centres without proper public oversight. To address these challenges, coordinated efforts among regulators, industry stakeholders, and academic institutions are required to ensure the reliable and proper adoption of technology in the security sector.

Recommendations

The literature reveals critical research gaps that require scholarly attention in South Africa's private security sector. It is recommended that future research and policy development focus on four key areas. First, a thorough legal review is necessary to update regulations, such as the PSIRA Act 56 of 2001, to address new technologies like AI and biometrics while protecting the public's rights. Second, in a country with high crime rates, studies should evaluate the effectiveness of these technologies in reducing crime in South Africa by using reliable data and methods. Third, research should explore how access to security technologies varies across communities and whether this deepens social inequality. Lastly, there is a need to assess current training programmes and develop inclusive strategies to equip security personnel with the digital skills required for modern security operations.

Limitations and Future Research

This study analyses documents and interprets their content, which is useful for understanding how technology and governance interact. However, it does not measure whether private security actually reduces crime or improves services by deploying advanced technologies. Future research should independently test effectiveness by tracking outcomes over time and comparing different areas. Studies should measure crime rates, the speed of security response, the frequency of false alarms, and whether services are equitable across all communities (Welsh and Farrington 2009; Lab 2016). There is a need for more research on whether biometric technology treats people fairly, how companies report cyberattacks, and how organisations can better coordinate their workflows, roles, and data practices.

References

Aale, L, Ylipulli J., Foth M., and Aurigi. 2023. “A. Urban AI: Understanding the Emerging Role of Artificial Intelligence in Smart Cities.” *AI and Society* 38(3): 1039–1044.

Ahmed, S., Qin X., and Martínez L. 2019. “Technological Anxiety and Job Security in the Digital Age.” *Journal of Security Studies* 12(3): 45–59.

Berg, J. and Nouveau J. 2021. “Towards Responsive Regulation of Private Security in South Africa.” *Criminology and Criminal Justice* 21(4):456–473.

Berg, J. 2020. “Private Security and Public Safety in Post-apartheid South Africa.” *Security Studies* 29(4): 678–704.

Biometric Update. 2023, May 12. “South Africa to Expand Biometric Border Control System.” https://www.biometricupdate.com/202305/south-africa-to-expand-biometric-border-control-system

Biometric Update. 2024, February 16. “Africa Border Security Week.” https://www.biometricupdate.com/202402/africa-border-security-week

Braun, V., and Clarke V. 2022. *Thematic Analysis: A Practical Guide.* 2nd ed. London: Sage Publications.

Bridges, L, Moyo T., and Sibanda N. 2018. “Organisational Barriers to Effective Security Implementation.” *Journal of African Management* 6(2):33–47.

Brudner, G. 2024. “Surveillance and Beyond: How Autonomous Indoor Drones Address Security and Operational Challenges.” https://www.securityindustry.org/2024/03/19/surveillance-and-beyond-how-autonomous-indoor-drones-address-security-and-operational-challenges/

Bulbulia. 2024. “Vumacam Partners with Gauteng Government to Provide Surveillance Access.” https://www.engineeringnews.co.za/article/vumacam-partners-with-gauteng-government-to-provide-surveillance-access-2024-02-13

Button, M. 2023. “Private Security in South Africa: A Comprehensive Analysis.” *Security Journal* 36(2): 234–251.

C-Drones. 2023, November 29. “Surveillance Security Drones South Africa | Customized Features.” https://c-drones.com/za/shop/advanced-security-drones-south-africa/

Caluza, L. 2022. “Smart Surveillance and Private Security in South Africa.” *Journal of African Security* 15(1):22–34.

Chibunna, U.B., Hamza O., Collins A., Onoja J.P, Eweja A., and Daraojimba A.I. 2020. “Building Digital Literacy and Cybersecurity Awareness to Empower Underrepresented Groups in the Tech Industry.” *Int. J. Multidiscip. Res. Growth Eval* 1(1):125–138.

Clarno, A. 2013. “Rescaling White Space in Post-apartheid Johannesburg.” *Antipode* 45(5):1190–1212.

Dagada, R. 2024. *Security Posture and Digital Transformation.* Johannesburg: Wits Press.

Dickinson, L.A. 2011. “Privatization and Accountability.” *Annual Review of Law and Social Science* 7(1):101–120.

Drone Guards. 2025, February 14. “Home - Drone Guards.” https://droneguards.africa/

Drone, D.J. 2021, May 25. “On-demand Private Security Drones Take Off in South Africa.” https://dronedj.com/2021/05/25/private-security-drones-south-africa/

Drozdowski, P., Rathgeb C., Dantcheva C., Damer N., and Busch C. 2020. “Demographic Bias in Biometrics: A Survey on an Emerging Challenge.” *IEEE Transactions on Technology and Society* 1(2): 89–103.

European Commission. 2021. *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence.* Brussels: European Commission.

European Parliament and Council. 2016. “Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data” (General Data Protection Regulation). *Official Journal of the European Union* L119/1.

Fahad, M, Anwar M., and Nawaz R. 2022. “Artificial Intelligence in Private Security: Current Trends and Future Prospects.” *Journal of Security Technologies* 15(3)”45–61.

Flytbase. 2025, May 2. “How 24-7 Drone Force Secures Residential Estates using Autonomous Drones in South Africa.” https://www.flytbase.com/case-studies/24-7-drone-force-residential-estate-security-docks-south-africa

Furnell, S. and Shah J. 2020. “Global Cybersecurity Skills Gap: A Critical Review.” *Computers and Security* 92: 101760.

G4S Risk Management. (n.d.). “Electronic Security Systems.” https://www.g4sriskmanagement.com/what-we-do/our-services/electronic-security-systems

Gumedze, S. 2015. “Promoting Partnerships for Crime Prevention between State and Private Security Providers in Southern Africa.” https://idl-bnc-idrc.dspacedirect.org/server/api/core/bitstreams/258025cc-7bc7-428f-894f-ecc9eb32985c/content

Institute for Security Studies. (n.d.). “Artificial Intelligence Regulation in South Africa – Prioritising Human Security.” https://issafrica.org/iss-today/artificial-intelligence-regulation-in-south-africa-prioritising-human-security

Kumar, A., Singh R., and Patel D. 2023. “IoT-Enabled Security Systems in Private Security: Innovations and Challenges.” *Security Technology Review* 8(1):21–36.

Lab, S.P. 2016. *Crime Prevention: Approaches, Practices, and Evaluations*. 9th edn. London: Routledge.

Micheal, D. 2025. "Secure and Intelligent Digital Environments: Leveraging APIs, IoT, Drones, and Machine Learning to Protect Critical Systems and Information Flows. https://www.researchgate.net/profile/Dave-Micheal/publication/392521684_Secure_and_Intelligent_Digital_Environments_Leveraging_APIs_IoT_Drones_and_Machine_Learning_to_Protect_Critical_Systems_and_Information_Flows/links/6846fde4df0e3f544f5dc1ac/Secure-and-Intelligent-Digital-Environments-Leveraging-APIs-IoT-Drones-and-Machine-Learning-to-Protect-Critical-Systems-and-Information-Flows.pdf

MIT Technology Review. 2022, April 19. "South Africa's Private Surveillance Machine is Fueling a Digital Apartheid." https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/

Masike, M, Von Solms S., and Marnewick A. 2019. "Socio-technical Systems Cybersecurity Framework." *Information and Computer Security* 27(2): 233–272.

Masombuka, M. 2018. "Towards An Artificial Intelligence Framework to Actively Defend Cyberspace in South Africa." Doctoral dissertation, Stellenbosch University.

Mondela, K., and Sirera T. 2023. *Digital Competency in Physical Security.* Pretoria: HSRC.

Nam, T. 2019. "Technology Usage, Expected Job Sustainability, and Perceived Job Insecurity." *Technological Forecasting and Social Change* 138:155–165.

Nayak, R, Saldanha J.C, Shetty S., Smitha A.B, and Raju R. 2025. "Security and Privacy Issues in Drone-Enabled IoT Networks." In *Machine Learning for Drone-Enabled IoT Networks. Advances in Science, Technology and Innovation,* edited by Hassan J., Khalifa S., and Misra P. pp. 65–80. Cham: Springer. https://doi.org/10.1007/978-3-031-80961-3_4

Ngwenya, M., and Ngoepe M. 2020. "A Framework for Data Security, Privacy, and Trust in Consumer Internet of Things." *Assemblages in South Africa. Security and Privacy* 3(5): p.e122.

Nkhoma, M. T., and Agbenyegah A. T. 2021. "Enhancing Border Security through Public-Private Partnerships in South Africa." *International Journal of Innovation, Creativity and Change* 15(10): 123–140.

Norris, C., and Armstrong G. 1999. *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg.

Pear, C. 2025. "Cybersecurity Challenges in Drone-Based Systems." https://anvil.so/post/cybersecurity-challenges-in-drone-based-systems

Pence, J., Mohaghegh Z., Ostroff C., Kee E., Yilmaz F., Grantom R., and Johnson D. 2014, June. “Toward Monitoring Organizational Safety Indicators by Integrating Probabilistic Risk Assessment, Socio-technical Systems Theory, and Big Data Analytics.” In *Proceedings of 12th International Topical Meeting on Probabilistic Safety Assessment and Analysis* (PSAM12).

Phillips, R. 2022. *AI and Predictive Analytics in Private Security*. Cape Town: Security Futures Institute.

RPAS Consulting. 2021, March 13. “Drone Security Surveillance. Southern Africa.” https://rpas.co.za/security-surveillance/

Rahman, S., and Patel D. 2022. “Biometric Technologies in Private Security: An Overview.” *Journal of Security and Privacy* 9(4):55–70.

Rensburg, J., Eugeny C., Hennicks M., and Heyns M. 2023. “Job Insecurity in South Africa’s Private Security Sector.” *Journal of Occupational Psychology* 14(1): 12–29.

Smith, J., and Lee H. 2023. “The Role of Drones in Modern Private Security Operations.” *International Journal of Security Management* 12(2): 89–104.

South African Government. 2025. *National Security* Strategy (2024–2028). Pretoria: Government Communication and Information System. https://www.gov.za/sites/default/files/gcis_document/202507/redacted-national-security-strategy2024-2028.pdf (Accessed: 31 July 2025).

South African Police Service. 2025. Annual Performance Plan 2025/2026. https://www.saps.gov.za/about/stratframework/strategic_plan/2025_2026/SAPS_2025-26_APP_%2804_April_2025%29.pdf

Sutherland, C., and Jamieson R. 2021. “Surveillance, Security and Human Rights in Post-apartheid South Africa.” *Social Justice* 47(3-4): 89–112.

UJ-TRCTI. 2022. *Technology and Innovation in South Africa*. Johannesburg: University of Johannesburg.

Vermesan, O., and Friess P. (Eds.). 2013. *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems.* New York: River Publishers.

Warfield, D. 2012. “Critical Infrastructures: IT Security and Threats from Private Sector Ownership.” *Information Security Journal: A Global Perspective* 21(3): 127–136.

Welsh, B.C., and Farrington D.P. 2009. “Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-analysis.” *Justice Quarterly* 26(4):716–745.