EAST AFRICAN JOURNAL OF CRIME AND SECURITY

JOURNAL ARTICLE

VOLUME 1, ISSUE 2 | PAGES 44-54

Technology Type and Incident Resolution Effectiveness Among Private Security Providers in Nairobi's Industrial Area

Silas Muriira Killingo

Mike Kiplagat Chepkong'a

https://doi.org/10.66699/a45dmh62

ABSTRACT

This article examines the relationship between the type of security technology and the effectiveness of incident resolution among private security providers in Nairobi's Industrial Area. Using a mixed-methods design that combines a structured survey of 217 respondents with eight key informant interviews, the research finds that technology adoption in the sector is bifurcated: conventional instruments (CCTV, alarms, biometric access control) are near-universally adopted, while computationally advanced tools (AI-based surveillance, drones) remain only marginally adopted. Multiple regression analysis reveals that adoption prevalence does not predict operational contribution; surveillance cameras and AI-based surveillance produced the largest effects on incident resolution, despite vastly different adoption rates, while security drones showed a statistically insignificant effect despite low uptake. These findings suggest that the underadoption of AI-enabled surveillance reflects structural barriers (cost, regulatory ambiguity, personnel competence) rather than limited operational value, whereas drones suffer from poor workflow integration. The study argues that closing Nairobi's private security technology gap requires targeted investment in advanced systems rather than further diffusion of already-saturated conventional tools.

Keywords: Private security, security technology, technology adoption, incident resolution

This article is licensed under a Creative Commons Attribution (CC BY) license
https://creativecommons.org/licenses/by/4.0/

How to Cite:

Killingo, S. M., & Chepkong'a, M. K. (2026). Technology type and incident resolution effectiveness among private security providers in Nairobi's industrial area. *East African Journal of Crime and Security*, 1(2), 44–54. https://doi.org/10.66699/a45dmh62

1. INTRODUCTION

1.1 Background

Urban insecurity across sub-Saharan Africa has increasingly outpaced the capacity of public policing institutions, prompting a structural shift toward privatised security provision (Crawford, 2008; Abrahamsen & Williams, 2011; Paddy, 2006). This shift is not merely an administrative substitution of private for public actors; it is accompanied by a parallel technological transition in which surveillance, access control, and analytic instruments are positioned as the principal levers for improving detection, deterrence, and response (Guma & Monstadt, 2021). Nairobi exemplifies this pattern. As the country's commercial and logistical nucleus, the city has embraced smart-infrastructure initiatives that fold security technology into broader urban governance projects, while simultaneously contending with a private security sector that has expanded faster than the regulatory apparatus designed to govern it (Mkutu, 2007).

The Industrial Area, a dense concentration of manufacturing plants, warehousing, and customs-bond operations within the city, occupies a particular position in this narrative. It combines high-value, largely immobile assets with a workforce and client base that are acutely sensitive to disruptions in security provision, making it a natural site for interrogating how technology is actually deployed, rather than how it is imagined in policy discourse (Diphoorn, 2016). Across the continent, evidence on the diffusion of security technology within the private sector remains structurally uneven: conventional instruments, namely alarms, closed-circuit television, and, increasingly, biometric access control, diffuse relatively quickly, while computationally intensive tools such as artificial-intelligence-enabled analytics and autonomous aerial surveillance diffuse slowly, constrained by cost, connectivity, and an underdeveloped regulatory environment (Arakpogun, Elsahn, Nyuur, & Olan, 2020; Naatu, Selormey, & Naatu, 2025). Ethical and data-governance concerns compound this slow diffusion, particularly for tools whose operation depends on the continuous capture of biometric or locational data (Dhirani, Mukhtiar, Chowdhry, & Newe, 2023).

A separate but related body of scholarship has begun to interrogate not whether technology is adopted, but whether adoption translates into improved operational outcomes at all, and if so, for which technologies (Njoroge, Ogalo, & Ratemo, 2021; Te, Kadar, Brüngger, & Cvijikj, 2016). This question remains unsettled. Some evidence links modernised surveillance instruments to measurable reductions in loss and faster resolution of security incidents (Schönteich, 1999), while other findings caution that unmaintained or poorly integrated systems can create a false sense of security without a corresponding operational gain (Hodges, 2021). It is this second, outcome-oriented question, rather than the more general question of adoption, that motivates the present paper.

1.2 Problem Statement

Nairobi's Industrial Area has recorded a marked escalation in reported criminal activity, with year-on-year increases that outstrip those recorded in comparably dense commercial zones of the city (Diphoorn, 2016; Ruteere & Pommerolle, 2003). Public policing capacity in the area remains constrained by resourcing limitations and by an investigative model that has not kept pace with the tactics of contemporary offenders, a gap that has pushed both firms and residents toward private security providers as de facto guarantors of operational continuity. Yet the private security sector that has absorbed this demand is not internally homogeneous in its technological posture, and existing scholarship offers little clarity on which specific class of technology, conventional or computationally advanced, is actually associated with improved incident resolution once adoption occurs, as distinct from mere ownership or installation of a device (Ngure & Handa, 2024; Mokora, 2022).

This paper advances a specific and testable claim: within Nairobi's Industrial Area, technology adoption among private security providers is bifurcated, with conventional electronic instruments functioning as normalised operational infrastructure while computationally advanced instruments remain nascent and unevenly integrated; and it is the computational sophistication of a technology, rather than its prevalence, that predicts its marginal contribution to incident resolution effectiveness. The paper interrogates this claim using data drawn from one specific objective of a broader mixed-methods study: identifying the security technologies used by private security providers and quantifying their differentiated impact on incident resolution as a single, focal security outcome.

2. LITERATURE REVIEW

The scholarship on private security technology in African urban contexts converges on a paradox that this study treats as its point of departure. On one hand, the promise of technological modernisation is well rehearsed: intelligent surveillance and analytic systems are credited, in principle, with compressing the interval between threat detection and operational response, and with generating an evidentiary record that strengthens both deterrence and post-incident investigation (Guma & Monstadt, 2021; Schönteich, 1999). On the other hand, the empirical record of adoption within African private security markets tells a more constrained story, one in which the technologies that diffuse fastest are not necessarily those with the strongest evidentiary claim to operational effectiveness, but those that are cheapest to procure, easiest to maintain, and least entangled with regulatory uncertainty (Ngure & Handa, 2024; Arakpogun et al., 2020).

This divergence between the promise and the pattern of adoption is best understood as a function of three intersecting constraints rather than as evidence of institutional inertia alone. The first is structural: infrastructural limitations, including inconsistent power supply and uneven connectivity, raise the effective cost of operating computationally intensive systems well above their nominal purchase price, a dynamic that recurs across multiple African security and finance-technology markets and is not unique to Kenya (Naatu et al., 2025; Arakpogun et al., 2020). The second is regulatory: tools that depend on aerial operation or on the continuous capture of biometric and locational data intersect with legal frameworks for data protection and airspace governance that remain either underdeveloped or unevenly enforced, which raises the transaction cost of deployment independent of any technical merit (Dhirani et al., 2023; Mkutu, 2007). The third is human capital: even where advanced systems are procured, their operational value is contingent on a workforce trained to interpret and act on their outputs, and training investment in the Kenyan private security sector has lagged procurement (Odhiambo, 2021; Mokora, 2022).

Read together, these constraints imply that adoption prevalence is a poor proxy for operational contribution, a distinction that the existing Kenyan literature has not adequately separated. Studies of the sector's technological landscape, including work conducted specifically in Nairobi, converge on a picture of near-universal uptake of conventional electronic instruments alongside marginal uptake of more advanced ones (Mokora, 2022; Makori, 2021). This convergence is informative about diffusion but says comparatively little about which widely or narrowly adopted technologies are implicated in operational performance, since prevalence and effectiveness are conceptually and empirically distinct properties of a technology. Where the literature does examine effectiveness directly, findings diverge in ways that resist simple synthesis: some studies attribute observed cost-effectiveness in the Kenyan context to conventional instruments precisely because their long institutionalisation has produced mature operating procedures around them. Others locate the operational advantage in the analytic and predictive capacity of newer, computationally intensive tools, despite their limited current footprint (Njoroge et al., 2021; Te et al., 2016).

A further thread in the literature complicates any technology-centred account of security outcomes by foregrounding the human and organisational scaffolding around a device. Human-capital theorists argue that technological instruments are, at best, force multipliers whose effectiveness is bounded by the situational judgement, training, and discretion of the personnel who operate them, and that an uncritical technological determinism risks obscuring this dependency (Chege, 2021; Radebe, 2025). Complementary work on the ethics and governance of surveillance technology cautions that the deployment of increasingly capable instruments, particularly those built on biometric or locational data, is not a purely technical decision but one with distributive and rights-related consequences that firms and regulators have been slow to confront (Dhirani et al., 2023; Diphoorn, 2016). This governance dimension is consequential for the present study because it suggests that the technologies with the greatest analytic power, namely artificial-intelligence-enabled systems, are simultaneously the technologies most exposed to adoption friction, producing a structural tension between operational potential and practical deployability.

Taken as a whole, the literature substantiates three propositions that this paper carries forward empirically. First, conventional and advanced security technologies occupy structurally different positions in the adoption landscape of Kenyan private security firms, a pattern consistent with broader evidence from Africa on technology diffusion under infrastructural and regulatory constraints (Arakpogun et al., 2020; Naatu et al., 2025). Second, the relationship between a technology's adoption prevalence and its contribution to operational outcomes is not self-evident and requires direct empirical interrogation rather than inference from adoption rates alone (Schönteich, 1999; Hodges, 2021). Third, any credible account of technology's contribution to a specific outcome such as incident resolution must be read against the parallel literature on regulatory friction and human-capital constraint, since these mediate whether a technology's theoretical capability is realised in practice (Chege, 2021; Ojwang, Bor, & Machira, 2024). It is precisely this three-part gap, between adoption, capability, and realised outcome, that the present paper's empirical objective is designed to close.

3. METHODS

3.1 Research Design

A cross-sectional quantitative design was used to collect data at a particular period, which permitted statistical modeling of the relationship between technology type and incident resolution effectiveness (Mugenda & Mugenda, 2003). This convergent design was considered appropriate for an objective that is simultaneously measurable, in terms of adoption frequencies and modelled effects, and interpretively contingent, in terms of why particular technologies underperform or overperform relative to their prevalence.

3.2 Study Site and Population

The study was situated in Nairobi's Industrial Area, a mixed manufacturing, warehousing, and logistics zone housing several hundred registered enterprises and served by a competitive private security market. To preserve the confidentiality of the participating organisations, individual providers are not named in this paper; instead, sampled firms are referred to by an anonymised operational tier corresponding to their scale, namely Tier 1 (large-scale providers, characterised by national or international reach and a workforce exceeding approximately 1,100 employees), Tier 2 (medium-scale providers, with a workforce of roughly 100 to 1,000 employees and regional operations), and Tier 3 (small-scale providers, with fewer than 100 employees and localised service scope). The study population comprised security personnel, including guards, surveillance officers, and event security officers, employed by the sampled firms.

3.3 Sampling Strategy and Sample Size

A stratified random sampling procedure was used to allocate the survey sample proportionately across the three operational tiers, reflecting their approximate share of the population of registered private security firms in the study area. The overall sample size was derived using the standard finite-population correction procedure for probability samples, applied at a 95 per cent confidence level with a five per cent margin of error, yielding a final achieved sample of 217 survey respondents drawn from firms across all three tiers. Within each tier, firms were selected at random, and respondents within selected firms were sampled to reflect the relative distribution of guards, surveillance officers, and event security officers.

3.4 Data Collection Instrument

Quantitative data were collected using a structured questionnaire covering the type and duration of technology in use, the frequency of technological upgrading, and respondents' evaluative ratings of each technology's contribution to security outcomes, including incident resolution, on five-point scales. The content validity of the instrument was assessed prior to full administration, consistent with established procedures for establishing agreement among expert reviewers on item relevance (Lawshe, 1975), and its internal consistency was subsequently examined using standard reliability coefficients for multi-item scales (Cronbach, 1951).

3.5 Data Analysis

Quantitative data were analysed using descriptive statistics to characterise the prevalence, duration, and perceived reliance associated with each technology category. To evaluate the paper's central empirical objective, that is, the differentiated contribution of technology type to incident resolution effectiveness, a multiple linear regression model was estimated with a composite incident resolution effectiveness score as the outcome variable and adoption or reliance indicators for six technology categories, namely surveillance cameras, biometric access control, security drones, artificial-intelligence-based surveillance, GPS tracking, and alarm systems, entered as simultaneous predictors.

4. FINDINGS

4.1 Descriptive Profile of Technology Adoption

Adoption of security technology among the sampled providers was markedly uneven across categories. Surveillance cameras were universally adopted; alarm systems and biometric access control were adopted by a large majority of firms; GPS tracking was adopted by a substantial majority; and both security drones and artificial-intelligence-based surveillance registered low adoption. Reported reliance ratings closely tracked this adoption gradient, with conventional instruments rated as central to daily operations and computationally advanced instruments rated as peripheral or experimental. Table 1 summarises these descriptive patterns.

Table 1:

Descriptive Summary of Technology Adoption and Operational Reliance (N = 217)

Security Technology	Adoption Rate (%)	Mean Reliance Rating (1–5)
Surveillance cameras (CCTV)	100.0	4.7
Alarm systems	90.3	4.5
Biometric access control systems	83.4	4.2
GPS tracking systems	70.0	3.9
Security drones	22.6	2.1
Artificial-intelligence-based surveillance	8.3	1.8

Note. Sample comprised 217 survey respondents stratified across Tier 1 (20%), Tier 2 (30%), and Tier 3 (50%) providers, supplemented by eight key informant interviews.

The pattern in Table 1 is consistent with a two-tier technological landscape in which conventional electronic instruments have been fully absorbed into routine operating procedure, while computationally advanced instruments remain in an early, largely exploratory phase of deployment. Notably, this gradient was consistent across operational tiers: even Tier 1 providers, who reported the highest absolute investment in newer technologies, described their AI-based and drone systems as pilot or supplementary tools rather than as core operational infrastructure. Tier 3 providers, by contrast, reported almost no exposure to either technology, a pattern consistent with the capital intensity of computationally advanced systems, which place them beyond the reach of smaller operators regardless of perceived merit. This tiered asymmetry indicates that the underadoption documented at the sector level is not evenly distributed across firm size, and that any policy response calibrated to the sector risks overlooking the sharper capacity constraint facing its smaller providers.

Frequency-of-upgrade data reinforced this descriptive picture. Conventional instruments were upgraded on a routine, multi-year cycle consistent with mature operational infrastructure, whereas advanced systems were, for a substantial share of adopting firms, never upgraded after initial installation. This distinction matters because it separates two forms of underadoption that are easily conflated: non-adoption, in which a firm has not acquired a technology, and stagnant adoption, in which a firm has acquired a technology but has not sustained the investment needed to keep it operationally current. The data suggest that computationally advanced technologies in this sector suffer from both.

4.2 Empirical Findings

4.2.1. Technology Type Predicting Incident Resolution Effectiveness

The regression model estimating the contribution of technology type to incident resolution effectiveness was statistically significant overall and explained a substantial proportion of the variance in the outcome. As reported in Table 2, four of the six technology categories were significant, independent predictors of incident resolution effectiveness, while one, security drones, did not reach conventional significance thresholds despite comparatively low adoption.

Table 2:

Multiple Regression Results: Technology Type Predicting Incident Resolution Effectiveness

Predictor	B	SE	β	t	p
Surveillance cameras (CCTV)	0.311	0.067	0.412	4.64	< .001
Biometric access control systems	0.147	0.053	0.201	2.77	.006
Security drones	0.091	0.059	0.122	1.54	.127
AI-based surveillance	0.258	0.063	0.344	4.10	< .001
GPS tracking systems	0.134	0.058	0.181	2.31	.022
Alarm systems	0.189	0.055	0.237	3.44	.001
Constant	1.204	0.342	—	3.52	.001

Note. $R^2 = .64$, *Adjusted* $R^2 = .61$, $F(6, 210) = 41.87$, $p < .001$. *Outcome variable: composite incident resolution effectiveness score (1–5).*

Two features of this result are analytically important. First, the magnitude of the standardised coefficients does not track adoption prevalence: surveillance cameras and artificial-intelligence-based surveillance, an almost universally adopted technology and a marginally adopted one respectively, returned the two largest standardised effects on incident resolution, while biometric access control and GPS tracking, both moderately to widely adopted, returned smaller though still significant effects. Second, security drones, despite registering the second-lowest adoption rate in the sample, produced the weakest and only non-significant coefficient, indicating that low prevalence alone does not explain a technology's limited contribution; rather, its contribution appears tied to how the technology is used operationally once deployed.

4.2.2. Perceived Contribution of Technologies to Incident Resolution

Respondents' evaluative ratings of each technology's specific contribution to incident resolution, summarised in Table 3, corroborate the regression pattern.

Table 3:

Perceived Contribution of Security Technologies to Incident Resolution (Mean Ratings, 1–5)

Security Technology	Mean Rating
Surveillance cameras (CCTV)	4.6
AI-based surveillance	4.3
Alarm systems	4.2
Biometric access control systems	4.0
GPS tracking systems	3.9
Security drones	3.5

Surveillance cameras and artificial-intelligence-based surveillance received the highest mean ratings for their contribution to resolving incidents, followed by alarm systems and biometric access control, while GPS tracking and security drones received the lowest ratings.

5. DISCUSSION

The findings warrant a discussion that moves beyond simply confirming a positive association between technology and security outcomes, toward an argument about what kind of technological capacity matters. The regression evidence indicates that adoption prevalence is not synonymous with operational contribution, and this divergence has substantive implications for how the sector's technological trajectory should be interpreted. If conventional instruments were adopted primarily because they are cheap and easy to procure, and if their contribution to incident resolution were correspondingly modest, the sector's near-universal reliance on them could be characterised as a rational but conservative equilibrium, optimised for cost rather than performance. That is not, however, what the data show. Surveillance cameras have the highest adoption rate and one of the two largest effects on incident resolution, undermining any account that treats conventional adoption as merely a low-cost default disconnected from operational merit. The more defensible reading is that the sector has, in this one respect, adopted correctly: its most prevalent technology is also among its most consequential.

The more analytically interesting tension lies with artificial-intelligence-based surveillance, whose adoption is marginal but whose estimated contribution to incident resolution rivals that of the sector's most entrenched technology. This combination is difficult to reconcile with an account of technology adoption driven purely by demonstrated effectiveness; if effectiveness alone governed diffusion, artificial-intelligence-based tools would be expected to diffuse faster than the data indicate. Their persistent underadoption, despite this apparent effectiveness, is better explained as a structural failure of enabling conditions, principally cost, regulatory ambiguity around data-intensive and autonomous systems, and a shortage of personnel equipped to operationalise their outputs, than as a rational market judgement about their operational worth. Framed this way, the underadoption of artificial-intelligence-enabled surveillance should be read as a loss of efficiency for the sector rather than as evidence of prudent caution.

Security drones present a different and, in some respects, more troubling pattern. Unlike artificial-intelligence-based surveillance, drones exhibit low adoption and a statistically weak, non-significant contribution to incident resolution, suggesting that their limited uptake is not simply the product of an artificial constraint on an otherwise valuable technology. Instead, the evidence is more consistent with an argument that drone deployment in this operational context remains poorly integrated into incident-response workflows, such that even where firms have invested in the technology, its outputs are not yet translating into measurably faster or more effective resolution. This distinction matters for how policy and firm-level investment should be prioritised: treating all under-adopted advanced technologies as equivalent, and equally deserving of accelerated investment, would be a misreading of the evidence. The data instead support a differentiated position, in which continued investment in artificial-intelligence-enabled surveillance is empirically defensible on effectiveness grounds, while drone investment, at least as currently operationalised within the sector, requires prior resolution of integration and workflow barriers before its returns can be expected to materialise.

A further implication follows from the tiered asymmetry documented in the findings. Because capital-intensive systems are concentrated disproportionately among larger providers, any sector-wide gain in incident resolution attributable to artificial-intelligence-based surveillance will, in the absence of intervention, accrue disproportionately to firms that are already best-resourced, widening rather than narrowing the operational gap between large and small providers. This distributive consequence is rarely addressed in the adoption literature, which tends to treat the sector as a single analytic unit, yet it bears directly on the practical question of how policy or industry-level investment should be targeted if the objective is a sector-wide improvement in incident resolution rather than a widening of intra-sectoral inequality.

This argument also bears on the broader debate, prominent in the literature on private security, over whether technological instruments are properly understood as substitutes for, or complements to, human operational capacity. The persistence of high reliance ratings for conventional, human-mediated practices alongside strong technological effects on incident resolution suggests that the sector's most effective configuration is not a simple substitution of machines for guards, but a division of labour in which technology compresses the time to detection and evidentiary clarity, while human personnel remain responsible for interpretation, judgement, and physical response. Read this way, the sector's underinvestment in training for advanced technologies is not a peripheral implementation detail but a direct constraint on the very outcome this paper has examined, since a technology's contribution to incident resolution is jointly produced by its computational capability and the competence of the personnel who act on its output.

6. CONCLUSION

Returning to the problem with which this paper opened, the escalation of criminal activity in Nairobi's Industrial Area has pushed the burden of operational security substantially onto private providers, and the evidence presented here indicates that this burden is being met with a technological base that is both incomplete and, in its most advanced segment, disproportionately underused relative to its demonstrated value. The claim advanced at the outset, that technological sophistication rather than adoption prevalence predicts a technology's marginal contribution to incident resolution, is supported by the regression evidence and corroborated by informants' own accounts of where the sector's technological gains and limitations lie.

The practical implication is that closing the security gap identified in the problem statement is unlikely to be achieved simply by encouraging further uptake of already well-diffused conventional instruments. The more consequential intervention lies in removing the specific structural barriers, cost, regulatory clarity, and personnel competence, that currently prevent computationally advanced

technologies from being deployed at a scale commensurate with their demonstrated operational effect. Absent such intervention, Nairobi's Industrial Area is likely to remain served by a private security sector whose technological ceiling is set less by the limits of available technology than by the limits of the conditions under which that technology can be meaningfully operated.

DECLARATION

Conflict of interest

The authors declare no conflict of interest of any form regarding this work, and is, thus, their original work done independently.

REFERENCES

Abrahamsen, R., & Williams, M. C. (2011). Security beyond the state: Private security in international politics. Cambridge University Press. https://doi.org/10.1017/CBO9780511974441

Arakpogun, E. O., Elsahn, Z., Nyuur, R. B., & Olan, F. (2020). Threading the needle of the digital divide in Africa: The barriers and mitigations of infrastructure sharing. *Technological Forecasting and Social Change,* 161, 120263. https://doi.org/10.1016/j.techfore.2020.120263

Odhiambo, J. (2021). *Impact of Private Security Firms as an Alternative in Crime Prevention within Nairobi Central Business District, Nairobi County, Kenya* (Doctoral dissertation, Kenyatta University).

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297–334. https://doi.org/10.1007/BF02310555

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. Sensors, 23(3), 1151. https://doi.org/10.3390/s23031151

Schönteich, M. (1999). Fighting crime with private muscle: The private sector and crime prevention. *African Security Studies*, *8*(5), 65-75.

Paddy Hillyard. (2006). Policing Northern Ireland: Conflict, Legitimacy and Reform. By Aogán Mulcahy (Cullompton: Willan, 2006, i–xii + 1–228pp. £17.99 pb, £40.00 hb), *The British Journal of Criminology*, Volume 46, Issue 5, September 2006, Pages 950–951, https://doi.org/10.1093/bjc/azl055

Guma, P. K., & Monstadt, J. (2021). Smart city making? The spread of ICT-driven plans and infrastructures in Nairobi. *Urban Geography*, 42(3), 360–381. https://doi.org/10.1080/02723638.2020.1715050

Hodges, D. (2021). Cyber-enabled burglary of smart homes. *Computers & Security,* 110, 102418. https://doi.org/10.1016/j.cose.2021.102418

Diphoorn T. (2016). "Surveillance of the Surveillers": Regulation of the Private Security Industry in South Africa and Kenya. *African Studies Review*. 2016;59(2):161-182. doi:10.1017/asr.2016.31

Ngure, A. R., & Handa, S. (2024). Challenges of integrating surveillance technologies and security management by private security providers in Nakuru County, Kenya. *Reviewed Journal of Social Science & Humanities*, 5(1), 223-234.

Makori, O. R. (2021). Strategy Implementation and Performance of Selected Private Security Firms in Nairobi City County, Kenya. *European Journal of Business and Management*, *7*(34), 71-90.

Lawshe, C. H. (1975). A numerical method for assessing content validity. Personnel Psychology, 28(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Mkutu, K. A., & Sabala, K. (2007). Private Security Companies in Kenya and Dilemmas for Security. *Journal of Contemporary African Studies*, *25*(3), 391–416. https://doi.org/10.1080/02589000701662442

Mokora, M. B. (2022). I*nformation technology and crime control in Nairobi City County, Kenya* [Doctoral dissertation, Kenyatta University].

Mugenda, O. M., & Mugenda, A. G. (2003). Research methods: Quantitative and qualitative approaches. Acts Press.

Naatu, F., Selormey, F. S., & Naatu, S. (2025). Determinants of digital technology adoption in sub-Sahara Africa: Ghana. International Journal of Emerging Markets, 20(10), 4111–4133. https://doi.org/10.1108/IJOEM-09-2023-1503

Crawford, A. (2008). Plural policing in the UK: policing beyond the police. *Handbook of policing*, *2*, 147-181.

Njoroge, P. M., Ogalo, J. O., & Ratemo, C. M. (2021). Information system security practices and implementation issues and challenges in public universities. European Journal of Information Technologies and Computer Science, 1(5), 11–15. https://doi.org/10.24018/compute.2021.1.5.30

Ojwang, D. O., Bor, E. K., & Machira, A. (2024). Officers' perceptions on influence of selected factors on General Service Unit's capacity to contain terrorism in Kenya. European Journal of Development Studies, 4(6), 1–8. https://doi.org/10.24018/ejdevelop.2024.4.6.399

Radebe, V. J. S. (2025). *Evaluating the significance of the private security companies (PSCs) to South Africa's national security* (Doctoral dissertation, Stellenbosch: Stellenbosch University).

Ruteere, M., & Pommerolle, M.-E. (2003). Democratizing Security or Decentralizing Repression? The Ambiguities of Community Policing in Kenya. *African Affairs*, *102*(409), 587–604. http://www.jstor.org/stable/3518515

Te, Y., Kadar, C., Brüngger, R. R., & Cvijikj, I. P. (2016). Human versus technology: Comparing the effect of private security patrol and crime prevention information system over the crime level and safety perception: Research in progress. In ECIS 2016 Proceedings (Article 48). https://doi.org/10.3929/ethz-a-010688920