EAST AFRICAN JOURNAL OF CRIME AND SECURITY

JOURNAL ARTICLE

VOLUME 1, ISSUE 2 | PAGES 33-43

# Security Technology as Opportunity Reduction: A Qualitative Analysis of Situational Crime Prevention in Nairobi's Industrial Area

Mike Kiplagat Chepkong'a

https://doi.org/10.66699/nrq24e90

## ABSTRACT

This article examines how stakeholder accounts of emergent security technologies in Nairobi's Industrial Area correspond with Situational Crime Prevention Theory (SCPT). It undertakes a qualitative secondary analysis of eight verbatim key-informant excerpts reported in the parent study and deliberately excludes all quantitative findings. A hybrid theory-directed thematic analysis first mapped the material to the five SCPT families increasing effort, increasing risk, reducing rewards, reducing provocations and removing excuses and then identified cross-cutting conditions that shaped whether technology could perform those functions. Six themes emerged: surveillance, visibility, and detection risk; rapid response and intervention; target hardening and access restriction; human competence as an enabling condition; governance and resource constraints; and confidence, behavioural regulation, and security value. Surveillance-related keywords occurred in six of eight excerpts (75.0%), while rapid response and competence each appeared in three (37.5%). Direct correspondence with SCPT was highly asymmetrical: increasing risk dominated the corpus; increasing effort appeared only narrowly; and the remaining three families were weakly represented or absent. The article argues that security technology should not be treated as an autonomous crime-control input. Its preventive value arises when devices are embedded in capable guardianship, timely intervention and legitimate governance. The findings therefore extend SCPT from a catalogue-like reading of security devices towards a sociotechnical account of how opportunity reduction is operationally produced in private-security environments.

**Keywords:** situational crime prevention; private security; surveillance technology; opportunity reduction



**How to Cite:**

Chepkong'a, M. K. (2026). Security technology as opportunity reduction: A qualitative analysis of situational crime prevention in Nairobi's industrial area. *East African Journal of Crime and Security*, 1(2), 33–43. https://doi.org/10.66699/nrq24e90

# 1. INTRODUCTION

## 1.1.Background

Urban security is increasingly organised through hybrid arrangements in which public policing, private security and digital infrastructures operate together. This is especially visible in African cities, where commercial premises, logistics corridors and industrial estates often rely on private providers for guarding, access control, alarm response and surveillance. In Kenya, private security has developed alongside uneven public protection, urban inequality and the expansion of market-based security provision (Abrahamsen & Williams, 2006; Mkutu, 2007). Nairobi's technology-driven urban development has further intensified the role of digital infrastructures in governing risk (Guma & Monstadt, 2021). The analytical question is therefore not simply whether technology is present, but how particular technological arrangements alter immediate opportunities for offending.

Situational Crime Prevention Theory (SCPT) is well suited to that question because it shifts attention from distant causes of criminality to the immediate organisation of opportunities. Clarke (1980) conceptualised situational prevention as the deliberate manipulation of environments to make offending more difficult, risky or less rewarding. Contemporary applications commonly organise situational measures around five families: increasing effort, increasing risk, reducing rewards, reducing provocations and removing excuses. Much private-security work is inherently situational: controlling entry, monitoring space, verifying identity, detecting anomalies, documenting incidents and mobilising response. These practices seek to reshape the immediate decision environment rather than transform the offender's underlying disposition. However, device presence cannot demonstrate opportunity reduction. CCTV research indicates preventive effects that vary markedly by setting, system design and active management rather than arising from installation alone (Piza et al., 2019; Welsh & Farrington, 2009). Skogan (2019) likewise situates contemporary CCTV within wider technological and organisational systems. This distinction is important in Nairobi's Industrial Area, where high-value assets, mobile workforces, restricted compounds and complex logistics coexist with uneven technical capacity. In such environments, the mechanism linking a device to prevention can be interrupted by weak training, poor response protocols, high capital costs or contested data practices.

The qualitative material in the supplied study is therefore analytically valuable because it records how managers and clients describe technology in operation. The eight available key-informant excerpts refer to biometric entry, CCTV, perimeter alarms, artificial-intelligence surveillance, security drones, GPS tracking, live-feed cameras, facial recognition, remote sensors, training, response confidence, internal theft, privacy, airspace policy and investment. Rather than asking how often firms have adopted each device, this manuscript asks what preventive mechanism participants attribute to technology and whether those mechanisms correspond to SCPT.

## 1.2 Problem Statement and Claim

This manuscript addresses a conceptual and empirical slippage between technological adoption and situational prevention. Security practice frequently treats surveillance, biometrics, alarms or artificial intelligence as if acquisition itself produces deterrence. That assumption obscures the mechanism SCPT requires technologies should matter only insofar as they alter offender effort, risk, reward, provocation or rationalisation within a concrete setting. A camera that is not monitored, a biometric device that is poorly operated, or an alert that does not trigger timely intervention may be technologically present while remaining criminologically weak. Conversely, a familiar technology such as CCTV may be highly consequential when actively monitored, interpreted by competent personnel and connected to rapid response.

A second problem concerns the institutional conditions under which opportunity reduction becomes legitimate and operationally credible. Data-intensive security tools can increase visibility and traceability, yet they also create questions of privacy, proportionality, airspace regulation, investment and organisational competence. Big-data surveillance can amplify pre-existing surveillance capacities rather than operate as a neutral technological layer (Brayne, 2017). Ethical analyses of emergent

technologies similarly demonstrate that privacy, accountability and governance are integral to implementation rather than secondary concerns (Dhirani et al., 2023). In Kenya, private security operates within a broader field of plural security provision in which non-state actors are indispensable but remain embedded in public regulation and contested relations of authority (Abrahamsen & Williams, 2006; Ruteere & Pommerolle, 2003).

Accordingly, the objective of this article is to examine the connection between SCPT, and the qualitative responses reported in the parent study while excluding the quantitative strand. The paper makes a clear claim: emergent security technologies in Nairobi's Industrial Area acquire preventive force principally through the SCPT mechanism of increasing perceived risk, but their effectiveness is mediated by human competence, response integration and governance legitimacy; technology alone is therefore an incomplete unit of explanation. The analysis further tests the internal breadth of SCPT by asking whether the qualitative evidence supports all five situational families or is concentrated around surveillance-oriented mechanisms.

Absence is treated as analytically meaningful. If participants do not articulate reward reduction, provocation management or excuse removal when explaining technology, that silence helps define the limits of a technology-centred SCPT account. Rather than forcing every device into all five families, the analysis distinguishes direct, partial and unsupported correspondence. This produces a more discriminating theoretical test and identifies the organisational capabilities that must supplement classic opportunity-reduction categories.

## 2. LITERATURE REVIEW

SCPT is a mechanism-based theory of opportunity reduction, not a catalogue of security products. Its analytical strength lies in specifying how changes to the immediate environment can influence the anticipated costs and benefits of offending. Increasing effort encompasses target hardening and controlled access; increasing risk includes surveillance, guardianship, and improved probability of detection; reducing rewards seeks to deny, conceal, or remove attractive benefits; reducing provocations limits situational triggers; and removing excuses clarifies rules or reduces opportunities for rationalisation. Clarke's (1980) formulation is consequently compatible with technological security only where the device can be connected to a specific alteration in opportunity. The relevant causal object is not the camera, biometric reader or drone in isolation, but the situational change the technology helps produce.

Surveillance technologies appear particularly compatible with the "increased risk" family, yet the empirical literature cautions against equating visibility with prevention. Meta-analytic evidence on CCTV suggests that effects are contingent and uneven across settings (Piza et al., 2019; Welsh & Farrington, 2009). This implies that a theoretical explanation must move beyond a simple visibility thesis. Detection must be sufficiently credible to influence offender expectations, and observation must be linked to some capacity for intervention. Skogan (2019) therefore treats CCTV's future as bound up with technological integration, analytical capability and organisational use rather than camera proliferation alone. This logic is directly relevant to private security, where monitoring personnel, control rooms, mobile response teams and site guards can convert information into immediate action or fail to do so.

The same distinction applies to artificial intelligence and data-intensive surveillance. Automated pattern recognition can expand the volume and speed of observation, but the criminological mechanism remains mediated by how alerts are interpreted and acted upon. Brayne (2017) shows that data-intensive policing transforms surveillance by making it more systematic, predictive and scalable. Such capacities can increase perceived detection risk, yet they also redistribute discretion and create new forms of informational power. Dhirani et al. (2023) demonstrate that privacy and ethical dilemmas accompany emerging technologies, indicating that technological reach cannot be separated from questions of legitimate use. For SCPT, this creates a productive tension: a measure

may raise offender risk while simultaneously generating institutional or privacy risks that undermine adoption, legitimacy or sustained operation.

Private-security contexts sharpen this sociotechnical reading. Kenya's security landscape reflects the growing importance of private providers in protecting commercial and residential space (Abrahamsen & Williams, 2006; Mkutu, 2007), while plural-security arrangements leave unresolved questions of accountability and authority (Ruteere & Pommerolle, 2003). Nairobi's ICT-driven urban transformation further embeds technology within institutional and governance arrangements rather than treating it as an isolated upgrade (Guma & Monstadt, 2021). Security technology in an industrial district must therefore be interpreted as part of an organisational and regulatory assemblage.

This literature supports three propositions that guide the present analysis. First, technological security is theoretically meaningful when it can be mapped to a specific opportunity-reduction mechanism. Second, surveillance effects are likely to depend on the credibility of detection, interpretation and response rather than visibility alone. Third, competence and governance can condition whether a nominally preventive technology operates as such. These propositions also establish a gap. Existing technological-security research is often outcome-oriented, asking whether cameras or other systems reduce crime, whereas the supplied qualitative excerpts enable a mechanism-oriented question: how do actors themselves describe the pathway from technology to prevention?

The methodological literature reinforces an emphasis on patterned meaning rather than isolated quotation. Thematic analysis supports systematic identification of recurring interpretations while allowing theory-led and data-led coding to interact (Braun & Clarke, 2006, 2019). Trustworthiness requires transparent coding decisions and a clear distinction between description and interpretation (Nowell et al., 2017), while themes should answer the research question rather than merely reproduce interview topics (Kiger & Varpio, 2020). Accordingly, this study combines deductive SCPT coding with inductive attention to training, response integration, legitimacy and cost. It seeks theoretical inference about articulated and absent mechanisms, not statistical generalisation from eight excerpts.

## 3. METHODS

### 3.1 Research Design and Qualitative Corpus

This manuscript is a qualitative secondary analysis of the qualitative strand reported in a larger mixed-methods study conducted in Nairobi's Industrial Area. The parent study used key-informant interviews to obtain contextual accounts from actors involved in private security provision. The present article deliberately excludes surveys, correlations, regressions, and other quantitative material so the analysis remains focused on the connection between SCPT and the reported qualitative responses.

The available analytic corpus consisted of eight verbatim key-informant excerpts embedded in the parent study's findings. Four excerpts were labelled Corporate Security Managers (KII 1–4), and four were labelled Clients (KII 5–8). Elsewhere, the parent sampling plan listed four corporate security managers, two clients and two senior private-security guards. Because the excerpt labels and sampling-plan categories are not fully concordant, this manuscript follows the role labels attached to the quotations and does not infer, correct or reconstruct participant identities. This preserves data provenance and prevents an apparent reporting inconsistency in the source document from being silently resolved.

### 3.2 Confidentiality and Data Protection

Confidentiality was treated as a primary analytical constraint because operational security information can identify organisations or expose sensitive practices. No security company is named in this manuscript. The source study stratified providers by organisational size, so the neutral

descriptors Tier S, Tier M and Tier L are reserved for small-, medium- and large-provider discussion where organisational scale is relevant. Crucially, the available excerpts cannot be securely linked to those strata; no tier is therefore attached to an individual quotation. Participants are reported only as P1–P8, with broad manager/client roles retained where necessary for interpretation. Verbatim quotations are reproduced exactly as supplied, including grammatical irregularities, but all company identifiers are withheld.

### 3.3 Thematic Analysis and SCPT Mapping

Analysis followed a hybrid, theory-directed thematic approach. In the first pass, each excerpt was coded against the five SCPT families: increasing effort, increasing risk, reducing rewards, reducing provocations and removing excuses. A second inductive pass identified cross-cutting conditions not adequately represented by those five families, including staff competence, rapid-response integration, client confidence, regulatory legitimacy and resource constraints. Coding therefore used SCPT as a sensitising framework rather than as a template into which every statement had to fit. This approach is consistent with thematic analysis as an interpretive method that moves iteratively between patterned data and conceptual framing (Braun & Clarke, 2006, 2019).

To make thematic prominence transparent, keyword clusters were specified for each theme and their occurrence was assessed at excerpt level. The reported percentage is the proportion of the eight excerpts containing at least one keyword or phrase belonging to the relevant cluster ($n/8 \times 100$). Because an excerpt can contain several themes, percentages are intentionally non-exclusive and do not sum to 100%. They are descriptive indicators of recurrence within this bounded corpus, not estimates of population prevalence. The calculation is used to support not replace interpretive analysis.

Analytic trustworthiness was strengthened through an explicit codebook, retention of disconfirming and absent cases, separation of keyword coverage from theoretical claims, and preservation of the original wording of quotations. These procedures follow recommendations for transparent and credible thematic analysis (Nowell et al., 2017). The small, excerpt-based corpus constrains claims about saturation and transferability; consequently, the analysis makes mechanism-oriented theoretical inferences rather than claims about the prevalence of views among Nairobi security providers (Kiger & Varpio, 2020).

## 4. FINDINGS

The eight excerpts form a focused corpus centred on surveillance, access control, response and technological competence. Their defining pattern is whether technologies make people or events visible quickly enough to trigger action, giving the material a pronounced SCPT orientation towards increasing perceived risk. Preventive value is nevertheless conditional: privacy and airspace policy constrain adoption, high investment limits implementation, and guards require training for confident response. Client accounts also show visible technology operating as a signal of provider capability and reassurance even where a direct crime-prevention mechanism is not stated.

**Table 1:**

*Descriptive summary of the qualitative corpus*

| Dimension | Description | Analytic implication |
|---|---|---|
| Corpus | Eight verbatim KII excerpts reported in the supplied study. | Bounded secondary-analysis corpus; no population-prevalence claims. |
| Excerpt role labels | P1–P4: manager-labelled; P5–P8: client-labelled. | Role labels follow the quotations as reported. |
| Sampling-plan discrepancy | The parent plan separately lists 4 managers, 2 clients and 2 senior guards. | No attempt was made to infer or repair participant identities. |
| Technologies named | CCTV/cameras, biometric entry, perimeter alarms, AI surveillance, security drones, GPS tracking, facial recognition, remote sensors and smart technology. | The corpus spans access control, surveillance, tracking and analytics. |
| Implementation conditions | Training, operator capability, timely notification, response, privacy, airspace policy and investment. | Technology is described as embedded in organisational and regulatory conditions. |
| Confidentiality protocol | Company names withheld; participants coded P1–P8; firm-size tiers not attached to quotations. | Protects operational confidentiality and avoids unsupported re-identification. |

### 4.1 Theory-Directed Themes

Six themes organise the qualitative material. Surveillance visibility and detection risk is the dominant pattern, appearing in six of eight excerpts (75.0%). Rapid response and intervention appear in three excerpts (37.5%), as does human competence as an enabling condition. Confidence, behavioural regulation and security value appear in four excerpts (50.0%). Governance and resource constraints occur in two excerpts (25.0%), while direct target-hardening language is concentrated in a single excerpt (12.5%). These percentages indicate excerpt-level recurrence of pre-specified thematic keywords; because themes co-occur, they should be read as descriptive prominence rather than mutually exclusive categories.

**Table 2:**

*Theory-directed thematic matrix with verbatim evidence*

| Theme | Keyword cluster | Exact verbatim excerpt(s) | n(%) |
|---|---|---|---|
| Surveillance visibility and detection risk | surveillance; CCTV; cameras; facial recognition; sensors; identifying | P2: "AI surveillance and security drones are on our radar, we have had a series of pilot cases where they were more effective in terms of identifying security risks and notifying the security personnel's in time as opposed to native security apparatus, but their implementation is limited by the high investment needed." P7: "The presence of high-end tech like facial recognition and remote sensors gave us confidence in the firm's capability." | 6/8 (75.0%) |
| Rapid response and intervention | respond/response; incident resolution; notifying; in time | P4: "Since rolling out GPS trackers and live-feed cameras, our incident resolution time has improved by over 50%." P5: "I'm more reassured when the guards actually know how to operate the CCTV and can respond confidently during an incident." | 3/8 (37.5%) |

| Theme | Keyword cluster | Exact verbatim excerpt(s) | n(%) |
|---|---|---|---|
| Target hardening and access restriction | biometric entry; perimeter alarms | P1: "We've standardised on biometric entry, CCTV coverage, and perimeter alarms across all our contracts. However, we are reluctant to adopt new emerging AI security tool since mast of them such as security drones have questions regarding data privacy and airspace policy" | 1/8 (12.5%) |
| Human competence as enabling condition | e-learning; learn; operate; guards; capability; confidently | P3: "We've built an e-learning platform where guards learn to operate each technology before they're posted." P5: "I'm more reassured when the guards actually know how to operate the CCTV and can respond confidently during an incident." | 3/8 (37.5%) |
| Governance and resource constraints | privacy; policy; investment; limited; reluctant | P1: "However, we are reluctant to adopt new emerging AI security tool since mast of them such as security drones have questions regarding data privacy and airspace policy" P2: "...their implementation is limited by the high investment needed." | 2/8 (25.0%) |
| Confidence, behavioural regulation and security value | confidence; reassured; fewer internal thefts; better behaviour; feedback; selling point | P6: "With the new surveillance systems, we've noticed fewer internal thefts and better behaviour by casual staff." P8: "Our client feedback scores correlate directly with the presence of smart technology it's now a major selling point." | 4/8 (50.0%) |

**Note.** Percentages are excerpt-level keyword coverage (n/8 × 100). An excerpt can contribute to more than one theme. Quotations are reproduced verbatim from the supplied manuscript; grammatical irregularities are not corrected.

The first two themes reveal a linked sequence rather than separate technological effects. P2 describes artificial-intelligence surveillance as useful because it identifies risk and notifies personnel "in time"; P4 similarly connects live-feed cameras and GPS tracking with faster incident resolution. The mechanism is therefore temporal as well as visual. Technology extends the field of observation, but its preventive significance depends on converting visibility into timely mobilisation. P5 makes this chain explicit from the client perspective: reassurance depends not simply on CCTV but on guards knowing how to operate it and respond confidently during an incident.

Target hardening is present but comparatively narrow. P1's reference to biometric entry and perimeter alarms directly represents the restriction of access and physical/electronic strengthening of boundaries. Yet the same excerpt immediately introduces reluctance concerning newer AI tools because of privacy and airspace policy. This juxtaposition shows that increasing offender effort and expanding surveillance are not unconstrained technical choices; their use is filtered through regulatory acceptability.

Human competence cuts across device categories. P3's e-learning platform places training before deployment, positioning competence as an operational prerequisite rather than a remedial activity. Client confidence in P5 and P7 reinforces this reading. The data therefore distinguish technical possession from technological capability. A device can be installed without creating a credible situational barrier if staff cannot interpret its output or connect it to action.

Finally, P6 and P8 reveal consequences that sit partly outside classic SCPT language. P6 associates surveillance with fewer internal thefts and better casual-staff behaviour, suggesting behavioural regulation through perceived observation. P8 frames smart technology as a selling point linked to client feedback. These statements show that technologies also produce symbolic value: they

communicate capability to clients and shape organisational conduct. Such effects may reinforce security, but they should not be conflated automatically with direct crime prevention.

### 4.2 Correspondence with the Five SCPT Families

Direct mapping to the five SCPT families produces a distinctly uneven pattern. Increasing risk is the only mechanism with broad qualitative support, appearing in six excerpts (75.0%). Increasing effort is directly articulated in one excerpt (12.5%) through biometric entry and perimeter alarms. P6 indirectly suggests reducing rewards and reducing provocations, while removing excuses has no direct support in the available material. This asymmetry is theoretically important: participants overwhelmingly explain technological security through seeing, identifying, notifying, and responding rather than through benefit denial, provocation management, or rule clarification.

**Table 3:**

*Empirical correspondence between the qualitative evidence and SCPT mechanisms*

| SCPT | Qualitative indicator | Participants | Coverage n/8 (%) | Interpretive assessment |
|---|---|---|---|---|
| Increase effort | Biometric entry; perimeter alarms | P1 | 1/8 (12.5%) | Direct but narrow evidence of access restriction/target hardening. |
| Increase risk | CCTV; surveillance; AI identification; cameras; facial recognition; sensors; timely response | P1, P2, P4, P5, P6, P7 | 6/8 (75.0%) | Dominant mechanism: visibility is linked to detection and credible intervention. |
| Reduce rewards | Fewer internal thefts | P6 | 1/8 (12.5%) | Indirect/weak: an outcome is described, but reward denial or benefit removal is not explicitly articulated. |
| Reduce provocations | Better behaviour by casual staff | P6 | 1/8 (12.5%) | Partial/ambiguous: behavioural regulation is present, but classic provocation-management mechanisms are not specified. |
| Remove excuses | No direct rule-setting, instruction, compliance cue or offender rationalisation mechanism | | 0/8 (0.0%) | Unsupported in the available corpus. |

**Note.** Coverage is based on the eight available excerpts. The labels "indirect", "partial" and "unsupported" prevent over-fitting the data to the theoretical framework.

## 5. DISCUSSION OF FINDINGS

The central finding is that security technology is narrated primarily as an architecture of visibility. The dominant SCPT mechanism is not "technology" as such but the perceived probability that conduct will be seen, identified, documented and followed by intervention. This distinction matters because it

relocates the causal claim from the artefact to the opportunity structure. CCTV, live feeds, AI-enabled identification, facial recognition and sensors have preventive meaning when they make detection sufficiently credible to influence behaviour. The qualitative corpus therefore supports a mechanism-centred reading of SCPT: technological systems alter situations by changing what can be observed and how quickly that observation can be converted into consequence.

This interpretation is stronger than a generic claim that surveillance deters crime. The CCTV literature shows that preventive effects depend heavily on context and system operation (Piza et al., 2019; Welsh & Farrington, 2009). The present accounts supply an organisational explanation for that contingency. P2 links identification to timely notification; P4 links live-feed cameras and GPS tracking to incident resolution; P5 links CCTV to guards capable of confident response. Together, these statements describe a sequence of observability, interpretation and intervention. If any link fails, the technology may remain visible without increasing meaningful offender risk. Skogan's (2019) emphasis on integrated surveillance systems is therefore theoretically important because it shifts analysis from camera presence to the organisational production of credible detection.

The prominence of increasing risk also reveals an internal asymmetry within SCPT. Technology-centred security practice in this setting mobilises only a selective portion of the framework. Increasing effort appears in access-control measures, but reducing rewards, reducing provocations and removing excuses are not prominent ways participants explain technological security. This should not be read as evidence that those mechanisms are unimportant in Nairobi's Industrial Area. Rather, it indicates that the discourse and operational imagination surrounding emergent security technologies are surveillance heavy. The finding cautions against presenting technology adoption as a comprehensive instantiation of SCPT. A security strategy centred on detection may leave other opportunity-reduction pathways underdeveloped.

Human competence is the principal bridge between a device and a situational mechanism. P3's e-learning platform is particularly revealing because training occurs before guards are posted. Competence is therefore built into deployment, not appended after the fact. P5's reassurance when guards can operate CCTV and respond confidently further shows that clients evaluate security through the human-technology interface. From an SCPT perspective, this means capable operation is part of the causal chain that makes risk credible. The device extends sensory reach; the operator interprets information; procedures determine whether action follows. Treating training as an external organisational variable would therefore underestimate its criminological significance.

This argument also qualifies the meaning of client confidence. P7 and P8 show that high-end or smart technology can signal organisational capability and become a commercial selling point. Such reassurance may be valuable, but confidence is not equivalent to demonstrated prevention. A technologically impressive system can create symbolic security without altering offender opportunity if monitoring and response are weak. Conversely, a less novel technology can be situationally powerful when embedded in disciplined routines. The distinction guards against security theatre: the visible performance of sophistication should not substitute for evidence that a system raises effort or risk in practice.

Governance produces a second mediating condition. P1's reluctance regarding AI tools and security drones is explicitly tied to data privacy and airspace policy, while P2 identifies high investment as an implementation constraint. These are not peripheral barriers to an otherwise complete technological mechanism. They shape whether surveillance can be lawfully deployed, maintained and trusted. Dhirani et al. (2023) foreground comparable privacy and accountability dilemmas in emerging technologies, while Brayne (2017) demonstrates how data-intensive surveillance can amplify institutional reach. The resulting paradox is central to contemporary SCPT: a technology designed to raise the offender's perceived risk may also raise privacy and governance risks for legitimate users and organisations.

This governance problem is especially salient in Kenya's plural security field. The expansion of private security redistributes protective capacity beyond the state, but it does not remove questions

of accountability, authority and public legitimacy (Abrahamsen & Williams, 2006; Ruteere & Pommerolle, 2003). In Nairobi's wider digital transformation, technological infrastructures are similarly intertwined with institutional arrangements and urban governance (Guma & Monstadt, 2021). SCPT applications in private security should therefore incorporate legitimacy as an implementation condition. Opportunity reduction that cannot survive legal scrutiny, data-protection requirements or community trust is unlikely to remain operationally stable.

The findings suggest a sociotechnical extension of SCPT for technology-rich private security. Technological observability creates information; competent personnel interpret it; integrated procedures convert interpretation into intervention; and governance and investment sustain the system. Visible capability can also reassure clients. Only the first element resides in the physical device; the remainder depends on skills, routines and institutional permission. SCPT is therefore retained, but its operation is specified as organisationally mediated.

The analysis remains deliberately bounded. Eight published excerpts cannot establish technological effectiveness or prevalence, resolve displacement or offender adaptation, or represent variation between firms. The parent document also contains a discrepancy between its sampling plan and the role labels attached to quotations. These constraints preclude claims of representativeness but do not prevent mechanism-oriented inference. Across the corpus, prevention is consistently explained through visibility, competent use and response, while three of the five situational families receive little direct articulation. That asymmetry is the manuscript's central empirical contribution.

## 6. CONCLUSION

This qualitative re-analysis examined the connection between SCPT and stakeholder responses concerning emergent security technologies in Nairobi's Industrial Area. Increasing perceived risk is the dominant mechanism, expressed through CCTV, AI surveillance, cameras, identification, sensors and timely notification. Increasing effort appears through controlled entry and perimeter protection, whereas the other situational families receive little direct support. The central theoretical contribution is that visibility becomes preventive only when coupled with trained personnel and credible response.

For practice, procurement should be evaluated as a prevention system rather than a device inventory. Providers should ask whether a technology demonstrably raises effort or risk, whether alerts reach competent staff, whether incident protocols turn information into action, and whether data collection is lawful, proportionate and trusted. Training platforms such as the one described by P3 should be treated as security infrastructure rather than an optional human-resources add-on. Privacy, airspace policy and capital cost should similarly be built into technology selection at the design stage.

Future research should analyse full interview transcripts and deliberately sample for underrepresented SCPT mechanisms, especially reducing rewards, provocations and excuses. Comparative work across Tier S, Tier M and Tier L providers could then examine whether organisational scale changes how opportunity-reduction mechanisms are assembled, while preserving firm anonymity. The manuscript's claim is straightforward: security technology prevents situations by changing opportunity through a credible sociotechnical chain of detection, interpretation, and response; technological novelty by itself is not the mechanism.

## REFERENCES

Abrahamsen, R., & Williams, M. C. (2006). Security sector reform: Bringing the private in. *Conflict, Security & Development, 6*(1), 1–23. https://doi.org/10.1080/14678800600590595

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health, 11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Clarke, R. V. G. (1980). "Situational" crime prevention: Theory and practice. *The British Journal of Criminology, 20*(2), 136–147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

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

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

Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. *Medical Teacher, 42*(8), 846–854. https://doi.org/10.1080/0142159X.2020.1755030

Mkutu, K. (2007). The private security industry in Kenya: Issues and challenges. In T. Jäger & G. Kümmel (Eds.), *Private military and security companies: Chances, problems, pitfalls and prospects* (pp. 177–201). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-90313-2_12

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*, 1–13. https://doi.org/10.1177/1609406917733847

Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy, 18*(1), 135–159. https://doi.org/10.1111/1745-9133.12419

Ruteere, M., & Pommerolle, M.-E. (2003). Democratizing security or decentralizing repression? The ambiguities of community policing in Kenya. *African Affairs, 102*(409), 587–604. https://doi.org/10.1093/afraf/adg065

Skogan, W. G. (2019). The future of CCTV. *Criminology & Public Policy, 18*(1), 161–166. https://doi.org/10.1111/1745-9133.12422

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly, 26*(4), 716–745. https://doi.org/10.1080/07418820802506206