Sing. J. Bus. Eco. & Mng, 12(3)2026, 117-121
ISSN: 3009-0024
Open Access

Singaporean Journal of Business Economics and Management

Research Paper

Security technology expos, procurement realities and strategic barriers for developing-economy state-owned enterprises

Remone Govender (PhD)

Senior Manager: Security Solutions Physical, Group Investigation and Security, Eskom Holdings SOC Ltd, Johannesburg, South Africa.
Corresponding email: remone19@gmail.com

Abstract: Security technology exhibitions are promoted as gateways to innovation, knowledge transfer and vendor relationships. For developing-economy state-owned enterprises (SOEs), however, the value of these expos is more complicated than the marketing narrative suggests. Drawing on field observations from the China Public Safety Expo (CPSE) 2025, comparative analysis of major international security exhibitions and documentary review of South African procurement and security-governance sources, this article examines whether security expos produce operational value or mainly reproduce vendor spectacle. The analysis finds that expos do create real value by exposing security practitioners to emerging technologies, vendor ecosystems and global design trends. That value is nevertheless constrained by procurement rules, weak local support ecosystems, language and documentation barriers, technology-life-cycle uncertainty and geopolitical concerns around surveillance infrastructure. The paper argues that developing-economy SOEs should treat expos as structured intelligence-gathering platforms rather than direct procurement channels. It proposes a disciplined expo-to-implementation framework built around pre-attendance objectives, post-expo validation, local partner assessment, life-cycle support review and governance assurance.

Keywords: Security technology exhibitions; CPSE; procurement governance; state-owned enterprises; developing economies; surveillance technology; South Africa

Received: 11 Apr 2026 | Accepted: 27 Jun 2026 | Available Online: 10 Jul 2026

1 | INTRODUCTION

Security technology exhibitions have become important meeting points for vendors, integrators, consultants, regulators and end-users. Events such as the China Public Safety Expo (CPSE), ISC West, Global Security Exchange (GSX), International Security Expo and regional African security exhibitions are marketed as places where decision-makers can see the future of security in one concentrated environment. The promise is attractive: one trip, hundreds of suppliers, live product demonstrations, networking opportunities and direct exposure to technologies that may not yet be visible in local markets. That promise requires careful scrutiny. Security expos are not neutral knowledge forums. They are commercial environments designed to generate leads, promote vendors and shape purchasing preferences. Exhibition floors are curated to impress. Booths, demonstrations and keynote narratives emphasise innovation, speed and transformation. The deeper questions - whether the technology can be procured lawfully, supported locally, integrated into existing infrastructure and sustained over a full operational life cycle - are often pushed into follow-up conversations that never happen. For developing-economy state-owned enterprises (SOEs), the gap between expo enthusiasm and operational implementation is especially wide. A South African SOE may identify an attractive perimeter-detection system, artificial-intelligence video platform, biometric access-control solution or drone-detection capability at an international exhibition. Yet the organisation may be unable to convert that exposure into implementation because the vendor has no local presence, support material is not available in English, procurement rules favour local suppliers or specific transformation objectives, and security leadership cannot justify the life-cycle risk of unsupported foreign technology. This article examines that gap. It does not dismiss expos as empty marketing spectacle. The central argument is more nuanced: security expos provide real but conditional value. They are useful for technology intelligence, vendor mapping, benchmarking and strategic awareness. They are much weaker as direct procurement pathways for SOEs operating under public-sector governance, budgetary constraints and local supplier-development obligations. The article is guided by three questions. First, what substantive value do security technology expos provide beyond marketing and vendor promotion? Secondly, how do Asian exhibitions such as CPSE compare with Western security expos in terms of knowledge transfer, language accessibility, vendor engagement and implementation potential? Thirdly, what structural barriers prevent developing-economy SOEs from converting expo exposure into operational security improvement?

2 | METHODOLOGY AND SCOPE

The paper adopts a qualitative critical case-study approach. It draws on field observations from attendance at CPSE 2025, comparative documentary analysis of major security exhibitions and review of South African public-procurement and security-governance sources. The approach is deliberately practical rather than purely theoretical. The concern is not only what expos claim to offer, but what a public-sector security function can actually do with the information, contacts and technologies encountered at such events. The CPSE observations are treated as practitioner field notes. They are not presented as statistically representative of all exhibitors, attendees or technologies. Rather, they provide grounded insight into recurring engagement problems: translation gaps, vendor assumptions about direct purchasing, limited local support models, uncertainty about long-term spares and warranties, and difficulty aligning fast technology cycles with slow public procurement processes. The comparative component considers widely recognised security exhibitions, including CPSE, ISC West, GSX and International Security Expo. Public event information and organiser material are used cautiously because exhibition data is promotional by nature. Attendance figures, exhibitor numbers and venue scale are therefore treated as indicators of market positioning rather than as proof of value. The legal and governance component focuses on the South African SOE context. South African public entities operate within procurement and financial-management frameworks that are designed to promote accountability, fairness, transparency, transformation and value for money. These frameworks include the Public Finance Management Act 1 of 1999, the Preferential Procurement Policy Framework Act 5 of 2000, the Preferential Procurement Regulations, 2022 and National Treasury guidance on implementation. For security functions, these frameworks matter because the most technically attractive solution is not always the solution that can be lawfully or practically procured. The study has limitations. It does not calculate a financial return on expo attendance. It does not test vendor products. It does not independently audit all event statistics. Its contribution lies in developing a structured, governance-aware framework for evaluating expo value from the perspective of developing-economy SOEs.

3 | LITERATURE AND GOVERNANCE CONTEXT

3.1 | Security technology, private security and surveillance

Security technology has become central to the governance of public and private space. Contemporary physical protection systems combine barriers,

sensors, access control, video surveillance, analytics, alarms, communications, command centres and response protocols (Garcia, 2008). The security function has therefore moved beyond guarding alone. It increasingly depends on integrated technology architectures that generate data, trigger decisions and shape organisational control. The growth of private and hybrid security governance is well documented. Abrahamsen and Williams (2011) argue that security increasingly operates beyond the state, while Button (2007) examines the powers, culture and control of private security officers in governed spaces. In South Africa, the relationship between public order, private security and state capacity has been examined by Minnaar (2005), Singh and Kempa (2007), and Berg and Nouveau (2011). This literature is important because SOEs often operate in the grey zone between public accountability and operational security imperatives.

Surveillance technology also raises difficult questions. CCTV may reduce certain crime risks, but its effectiveness depends heavily on context, monitoring quality and response capability (Welsh & Farrington, 2009). Surveillance systems also structure data, visibility and organisational power (Lyon, 2003; Flyverbom & Murray, 2018). Where surveillance technology is imported from foreign vendors, further issues arise around data sovereignty, cybersecurity, supplier influence and long-term dependence. Literature on Chinese surveillance infrastructure and state security technologies highlights why technology-source decisions may be politically and operationally sensitive (Hoffman, 2020; Liang et al., 2018; Xu, 2021).

3.2 | Procurement governance and the SOE environment

SOEs do not purchase security technology in the same way as private corporations. A private company may identify a preferred vendor, conduct due diligence, negotiate terms and implement quickly. A South African SOE must align procurement decisions with statutory duties, internal delegations, audit requirements, preference-point systems, transformation objectives and supply-chain controls. The PFMA requires public resources to be managed efficiently and effectively, while also imposing duties of financial discipline and accountability (Public Finance Management Act 1 of 1999). The PPPFA and the Preferential Procurement Regulations, 2022 require organs of state to apply preference-point systems and set procurement-specific goals within the applicable legal framework (Preferential Procurement Policy Framework Act 5 of 2000; Preferential Procurement Regulations, 2022; National Treasury, 2023). This framework serves legitimate public purposes. It prevents arbitrary purchasing, supports transparency, and advances economic and transformation objectives. Yet it also creates implementation friction when the most suitable security technology is supplied by an international vendor without domestic representation, local service capability, transformation credentials or rand-based commercial arrangements. The difficulty is not simply bureaucratic inconvenience. It is structural: global security technology markets move quickly, while public procurement moves slowly and must satisfy purposes beyond technology performance alone. South Africa's procurement environment is also shaped by the history of corruption, state capture and public-sector procurement abuse. The State of Capture report and subsequent state-capture literature demonstrate why procurement governance cannot be treated as a mere administrative formality (Bhorat et al., 2017; Public Protector, 2016). For SOEs, the challenge is therefore double-edged. Security teams need access to modern technology, but procurement shortcuts create legal, audit and reputational risk.

3.3 | Expos as commercial knowledge environments

Security expos are hybrid spaces. They are partly professional-development forums, partly market-intelligence platforms and partly sales theatres. Organisers promote them as opportunities to discover innovation, attend technical sessions and meet vendors. Vendors use them to launch products, test market interest, collect leads and influence buyer preferences. Attendees use them to learn, compare, benchmark and sometimes validate pre-existing procurement intentions. This mixed character explains why expo value is uneven. A technically skilled attendee with clear objectives can extract serious intelligence from an exhibition floor. An unfocused delegation may leave with brochures, photographs and excitement but no implementable plan. The value of expo attendance therefore depends less on the size of the exhibition and more on the discipline with which the organisation prepares, documents, tests and follows up after the event.

4 | THE COMPARATIVE SECURITY EXPO LANDSCAPE

The major international security exhibitions differ in geography, audience, vendor profile and practical usefulness. CPSE is strongly associated with Asian manufacturing depth, rapid product iteration and Chinese surveillance, access-control and smart-security ecosystems. ISC West provides concentrated exposure to the North American security market and major Western manufacturers. GSX, powered by ASIS International, is more leadership and security-management oriented. International Security Expo in London positions itself around government, critical infrastructure, counter-terrorism and resilience audiences. These differences matter for developing-economy SOEs. A security delegation looking for tactical product awareness may derive strong value from CPSE because of the density and variety of technology. A delegation focused on governance, enterprise security management and strategic risk may find GSX more relevant. A delegation concerned with critical infrastructure, resilience and government-industry interface may benefit from London-based security events. No exhibition is inherently superior; each serves a different purpose. Scale is therefore a poor proxy for value. A very large exhibition may overwhelm attendees, fragment attention and make meaningful technical engagement difficult. A smaller, better-curated exhibition may produce higher-quality conversations. For a public entity with limited travel funds, the correct question is not 'which expo is the biggest?' but 'which expo best answers the organisation's current security questions?'

Table 1. Comparative value of selected security exhibitions for developing-economy SOEs

Expo type	Indicative strength	Main limitation for SOEs	Best use
CPSE / Asian manufacturing exhibitions	Breadth of hardware, surveillance, access-control and integrated platform vendors	Language barriers, limited local support, geopolitical and data-sovereignty concerns	Technology scanning and vendor landscape intelligence
ISC West / North American commercial security exhibitions	Strong access to established Western vendors, product launches and integrator ecosystem	High travel cost and Western-market assumptions about budgets and infrastructure	Benchmarking, product validation and vendor comparison
GSX / security-management exhibitions	Strategic security management, leadership and risk discussion	Less useful for detailed product procurement and technical testing	Security strategy, governance and professional development
International Security Expo / critical-infrastructure exhibitions	Government, resilience, counter-terrorism and infrastructure protection themes	Solutions may assume mature market support ecosystems	Critical infrastructure and policy-oriented learning

Note. The table is analytical and based on the paper's comparative review; it is not a ranking of expo quality.

5 | WHAT EXPOS ACTUALLY OFFER

5.1 | Technology exposure

The strongest defensible benefit of expo attendance is technology exposure. A security practitioner can see emerging categories, compare competing vendors, observe interface design, ask questions and identify solutions that may not yet be visible through local suppliers. This matters for SOEs whose security functions may be under-resourced and operationally consumed by immediate incidents. Expos create concentrated time for scanning the horizon. The limitation is depth. Exhibition demonstrations are designed to impress. Systems are shown under controlled conditions, with clean data, ideal lighting, reliable connectivity and vendor staff guiding the narrative. The real operational questions are harder: How does the system perform in dust, rain, heat, poor lighting or unstable networks? What happens when a firmware update fails? Can it integrate with legacy access control? Who repairs it at 02:00? What does it cost over 10 years? These questions are rarely answered fully at the booth.

5.2 | Vendor identification

Expos also help identify vendors and categories of suppliers. This is useful where local markets are thin or where existing suppliers recycle the same products. Field observations at CPSE 2025 confirmed that many vendors offer technically interesting solutions that would be relevant to infrastructure protection, cable-theft prevention, perimeter detection, video analytics and control-room integration. Identification is not the same as adoption. A vendor may have an impressive product but no local office, no South African integrator, no English technical manuals, no warranty process outside China and no ability to comply with SOE tender requirements. In that situation, the product is not yet a viable solution. It is a technology lead requiring further market-development work.

5.3 | Benchmarking and professional learning

Expo attendance can also sharpen professional judgement. Delegates learn how other markets talk about risk, how vendors package solutions, what terminology is emerging and what capabilities are becoming standard. This benchmarking value is real, especially for organisations that otherwise rely

heavily on local suppliers for market intelligence. The danger is uncritical transplantation. A technology strategy designed for a well-funded Western corporation, a Chinese smart-city programme or a high-density transport hub may not suit a South African SOE with budget limits, procurement constraints, bandwidth limitations and severe maintenance backlogs. Benchmarking must therefore be translated into local operational reality.

6 | BARRIERS TO TRANSLATING EXPO EXPOSURE INTO SOE IMPLEMENTATION

6.1 | Language and technical documentation

Language is one of the most underestimated barriers in Asian security-technology engagement. Major vendors at CPSE may provide English-speaking representatives, but booth-level English capability is not the same as implementation readiness. Detailed technical specifications, installation manuals, configuration guides, training material and support documentation may be available only in Mandarin or in weak translation. This becomes critical during implementation. Security systems require precise configuration. Ambiguous translation in an access-control system, video-management platform or intrusion-detection device can cause commissioning errors, operational instability or unsafe workarounds. A brochure can be translated quickly; a complete engineering support ecosystem cannot. Western exhibitions have an advantage for English-speaking SOEs because technical documentation, training material and support conversations are generally more accessible. That advantage may justify higher attendance and technology costs where the alternative is a cheaper system that cannot be confidently installed, maintained or audited.

6.2 | Procurement and preference constraints

The second barrier is procurement. South African SOEs cannot simply buy what they see. Procurement must follow approved processes, preference-point systems, internal delegations and audit requirements. Where a foreign vendor has no local presence, local partner or compliant commercial structure, the technology may be practically unavailable even if it is technically suitable. This creates a paradox. Security professionals may be encouraged to attend international expos to identify innovation, but the procurement framework may prevent direct adoption of that innovation. The result is organisational frustration: the security function knows what may work, but the supply-chain route cannot easily deliver it. The problem is aggravated when evaluation models overemphasise upfront price. Security technology should be assessed on total life-cycle value, including performance, support, spares, integration, training, cybersecurity, warranty, local response capability and upgrade path. A lowest-price solution that fails after two years is not cheaper. It is deferred risk.

6.3 | Vendor market-entry and support sustainability

Field observations at CPSE 2025 revealed a recurring market-entry gap. Some vendors were interested in selling to South African entities but had limited understanding of SOE procurement, local support requirements or transformation-related supplier expectations. Several assumed that a customer could simply order directly from China and receive remote support. That model is insufficient for mission-critical infrastructure security. Complex security systems require site assessment, local installation, integration, commissioning, user training, emergency support, spare parts and long-term maintenance. Remote email or video support is useful, but it cannot replace a competent local integrator where the system controls access to a power station, logistics site, warehouse or command centre. Vendor sustainability also matters. Many technology vendors operate on short innovation cycles. Products are refreshed, discontinued or replaced quickly. SOEs often expect systems to remain operational for 10 to 15 years. If spares are discontinued after a few years or software updates stop, the organisation inherits a stranded asset. Expo evaluation must therefore include life-cycle interrogation, not only product demonstration.

6.4 | Geopolitics, cybersecurity and data sovereignty

Security technology is no longer politically neutral. Surveillance platforms, access-control systems, cloud video analytics, facial recognition and command-centre platforms generate sensitive operational data. For SOEs responsible for critical infrastructure, technology-source decisions may implicate national security, data protection, cybersecurity and foreign-policy considerations. The geopolitical debate around Chinese technology illustrates the issue. Literature on Chinese digital governance and surveillance infrastructure highlights the strategic importance of data, platforms and state-linked technology ecosystems (Hoffman, 2020; Liang et al., 2018; Xu, 2021). This does not mean that every Chinese technology is unsafe, nor that Western technology is automatically secure. It does mean that SOEs must ask hard questions about data location, remote access, source-code assurance, firmware updates, cloud hosting, supplier ownership and foreign-government access laws. On-premises deployment may reduce some data-sovereignty risks but may also limit advanced analytics that vendors increasingly offer through cloud platforms. The decision is therefore not only technical. It is a governance decision requiring risk appetite, legal review, cybersecurity assessment and executive approval.

Table 2. Expo-to-implementation barriers for developing-economy SOEs

Barrier	How it appears at expo stage	Operational implication	Required control
Language and documentation	Sales discussion possible, but technical manuals incomplete or poorly translated	Configuration, training and maintenance become unreliable	Require complete English technical documentation before shortlisting
Procurement compliance	Vendor has no local presence or compliant partner	Technology cannot be lawfully or practically procured	Conduct early supply-chain and legal screening
Support sustainability	Remote support offered instead of local response	Long outages and dependence on foreign engineering teams	Require local support model, SLA and spare-parts plan
Life-cycle risk	Product roadmap unclear or fast replacement cycle	Premature obsolescence and stranded assets	Assess warranty, spares, upgrades and end-of-life policy
Cybersecurity and data sovereignty	Cloud analytics or remote vendor access promoted without clarity	Sensitive infrastructure data may be exposed	Require cyber, privacy and data-sovereignty assessment
Marketing overstatement	Demonstrations occur in ideal conditions	Performance expectations become unrealistic	Mandate pilots and reference-site validation

7 | A GOVERNANCE-AWARE FRAMEWORK FOR EXPO ATTENDANCE

Developing-economy SOEs should not abandon expo attendance. They should professionalise it. Expo attendance should be treated as a formal intelligence and capability-development exercise, not as a reward trip, generic networking opportunity or unstructured market visit. The following framework is proposed.

7.1 | Pre-attendance discipline

Before attending, the organisation should define no more than five priority intelligence questions. These may include perimeter detection, control-room integration, drone detection, cable-theft prevention, access-control modernisation or AI-enabled video analytics. Each delegate should know what information to collect, what questions to ask and which operational problems the technology must solve. Delegation composition should be purposeful. A strong delegation should include technical security expertise, procurement insight, legal or governance awareness and cybersecurity capability. Sending a large delegation without clear roles is poor value. Sending a small delegation with disciplined objectives is far more defensible.

7.2 | Booth engagement discipline

At each relevant vendor engagement, delegates should record the same core information: product capability, integration requirements, local presence, installation model, support model, warranty period, spare-parts availability, cybersecurity posture, data-hosting model, references and willingness to work through a local partner. This creates comparable intelligence rather than a folder of unrelated brochures. Delegates should be sceptical of demonstrations. They should ask what happens in poor lighting, weak connectivity, high dust, high heat, vandalism, power interruption and system failure. These are not marginal questions for South African SOEs. They are operating conditions.

7.3 | Post-expo validation

The most important work begins after the expo. Promising technologies should be placed into a structured validation pipeline. The first filter is legal and procurement feasibility. The second is technical feasibility. The third is local support feasibility. The fourth is cybersecurity and data-sovereignty review. Only after those filters should a technology be considered for pilot or procurement planning.

SOEs should also seek reference checks and peer-site validation. A vendor demonstration is not enough. The organisation should speak to customers who have implemented the system under comparable conditions. If no reference sites exist in similar markets, the risk rating should increase.

7.4 | Local partner development

One practical way to bridge the gap between international technology and domestic procurement requirements is local partner development. SOEs should not select favourites or undermine competitive procurement. However, they can signal technology needs to the local market, host supplier information sessions and encourage capable domestic integrators to pursue partnerships with international vendors identified at expos. This approach supports both security modernisation and local capability development. It also shifts the vendor relationship from remote export sales to implementable local support. For SOEs, the question is not only whether the international vendor is impressive, but whether there is a credible domestic pathway to install and sustain the technology.

Table 3. Recommended expo governance cycle for SOEs

Stage	Decision discipline	Minimum output
Before attendance	Define priority problems, delegate roles and intelligence questions	Approved expo brief and collection template
During attendance	Collect comparable vendor information and test marketing claims	Vendor intelligence matrix
Immediate post-expo	Screen technologies for procurement, legal, support and cyber feasibility	Shortlist with risk ratings
Validation	Conduct demonstrations, reference checks and site/pilot testing	Technical and commercial validation report
Implementation planning	Confirm local partner, life-cycle costs, procurement route and assurance controls	Business case and procurement strategy

8 | IMPLICATIONS FOR SOUTH AFRICAN SOES

The implications for South African SOEs are direct. First, security functions should not rely on procurement teams to interpret technology value without technical input. Procurement governance is essential, but security effectiveness cannot be reduced to price and compliance scoring alone. Specifications must be informed by operational risk, not copied from vendor brochures or legacy tenders. Secondly, security technology acquisitions should be evaluated on total cost of ownership. This includes acquisition, installation, training, integration, software licensing, maintenance, spares, downtime, cyber assurance and eventual replacement. A superficially cheap system may be expensive when it fails, cannot be supported or cannot integrate with existing infrastructure. Thirdly, SOEs should create internal mechanisms to convert expo intelligence into strategy. After each major expo, the delegation should submit a formal report identifying trends, opportunities, risks, non-viable technologies and recommended follow-up actions. This report should go to security leadership, procurement, legal, IT/cybersecurity and finance. Without this governance loop, expo learning remains personal rather than institutional. Fourthly, SOEs should be realistic about Chinese technology. CPSE and similar exhibitions provide valuable visibility into rapidly developing security hardware and analytics ecosystems. However, adoption requires stronger due diligence on cybersecurity, data sovereignty, documentation quality, local support and long-term sustainability. The correct posture is neither blanket rejection nor uncritical enthusiasm. It is disciplined verification. Finally, policy reform should be considered where procurement processes unintentionally block legitimate security modernisation. This does not mean weakening accountability. It means creating evaluation models that give proper weight to quality, operational performance, life-cycle value, support capability and security risk. Where critical infrastructure protection is at stake, the cheapest compliant bid may still be the wrong answer.

9 | CONCLUSION

Security technology expos are valuable, but not in the simple way that exhibition marketing suggests. They are not magic procurement accelerators. They are intelligence environments. Their real value lies in exposing security practitioners to emerging capabilities, vendor ecosystems, design trends and comparative market options. That value becomes operational only when the organisation has the governance discipline to test, validate, procure and sustain what it has seen. For developing-economy SOEs, the barriers are substantial. Language gaps, weak technical documentation, absence of local support, procurement constraints, vendor market-entry hesitancy, life-cycle uncertainty and geopolitical risk all limit the direct adoption of expo technologies. These barriers do not make expo attendance pointless. They make unstructured expo attendance indefensible. The paper therefore argues for a more sober model of expo engagement. SOEs should attend selectively, prepare rigorously, document consistently and validate aggressively. They should treat vendor claims as hypotheses, not facts. They should ask not only whether a technology works, but whether it can be lawfully bought, locally supported, securely integrated, financially sustained and governed over its life cycle. The future value of security expos for developing-economy SOEs will depend on whether expos evolve beyond vendor spectacle and whether public entities mature beyond passive attendance. The opportunity is real. So is the risk of being dazzled by technology that cannot survive contact with procurement law, infrastructure constraints or operational reality.

Conflict of Interest
The authors declare that they have no conflict of interest regarding the publication of this manuscript.
Funding
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Author Contributions
All authors contributed significantly to the conception, design, data collection, analysis, and writing of the manuscript. All authors have read and approved the final version of the manuscript.
Informed Consent
Informed consent was obtained from all participants involved in this study prior to data collection.
Use of Generative AI
The authors confirm that generative AI tools were used only for minor language refinement and did not contribute to the intellectual content, analysis, or conclusions of the study.

REFERENCES

Abrahamsen, R., & Williams, M. C. (2011). Security beyond the state: Private security in international politics. Cambridge University Press.
ASIS International. (2025). GSX 2025 opens in New Orleans. ASIS International.
Berg, J., & Nouveau, J. (2011). Towards a third phase of regulation: Re-imagining private security in South Africa. South African Crime Quarterly, 38, 23-32.
Bhorat, H., Buthelezi, M., Chipkin, I., Duma, S., Mondi, L., Peter, C., Qobo, M., Swilling, M., & Friedenstein, H. (2017). Betrayal of the promise: How South Africa is being stolen. State Capacity Research Project.
Button, M. (2007). Security officers and policing: Powers, culture and control in the governance of private space. Ashgate Publishing.
Flyverbom, M., & Murray, J. (2018). Data structuring: Organizing and curating digital traces into action. Big Data & Society, 5(2), 1-12.
Garcia, M. L. (2008). The design and evaluation of physical protection systems (2nd ed.). Butterworth-Heinemann.
Hoffman, S. (2020). Programming China: The Communist Party's autonomic approach to managing state security. Mercator Institute for China Studies.
International Security Expo. (2026). International Security Expo: Event overview. Nineteen Group.
Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. Policy & Internet, 10(4), 415-453.
Lyon, D. (2003). Surveillance as social sorting: Privacy, risk, and digital discrimination. Routledge.
Minnaar, A. (2005). Private-public partnerships: Private security, crime prevention and policing in South Africa. Acta Criminologica, 18(1), 85-114.
National Treasury. (2023). Implementation guide: Preferential Procurement Regulations, 2022. Office of the Chief Procurement Officer.
Preferential Procurement Policy Framework Act 5 of 2000.
Preferential Procurement Regulations, 2022.
Public Finance Management Act 1 of 1999.
Public Protector. (2016). State of capture: Report on an investigation into alleged improper and unethical conduct by the President and other state functionaries. Public Protector South Africa.
RX Global. (2025). ISC West 2025 concludes, setting the stage for the future of security. RX Global.
Singh, A. M., & Kempa, M. (2007). Private security, public order: State outsourcing of police work and its implications. Theoretical Criminology, 11(2), 153-177.
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.
Xu, B. (2021). China's surveillance state: The technology behind mass control. Journal of Democracy, 32(2), 53-67.

Appendix A: Expo Intelligence Collection Template

Table A1. Minimum vendor information to collect during expo attendance

Field	Information to record
Vendor identity	Registered name, country, ownership, website, contact person and booth number
Technology category	Perimeter detection, CCTV, access control, VMS, drone detection, control room, cyber-physical integration or other
Problem fit	Which organisational security problem the solution may address
Technical requirements	Power, network, bandwidth, environmental tolerance, integration protocols and compatibility
Documentation	Availability and quality of English technical manuals, installation guides and training material
Local presence	South African office, partner, integrator, service agent or support plan
Support model	SLA, response time, remote support, on-site support and escalation process
Life-cycle assurance	Warranty, spares, software updates, end-of-life policy and upgrade path
Cyber/data issues	Cloud use, data location, remote access, encryption, audit logs and cybersecurity certifications
Procurement feasibility	B-BBEE/local partner options, contracting route and currency/payment constraints
Next step	Reject, monitor, request demo, seek local partner, pilot or include in strategy