# Mechanisms of Interaction Between Law Enforcement Agencies and Private Security Companies in Crime Prevention

[1] Kristijan Ilovača
[1] CEO of Sky Fort Systems d.o.o Croatia, Zagreb

Received: 20th Oct 2025 | Received Revised Version: 15th Nov 2025 | Accepted: 26th Nov 2025 | Published: 05stJan 2026

Volume 08 Issue 01 2026 | 10.37547/tajpslc/Volume08Issue01-02

## Abstract

*The article is devoted to the study of the evolution of mechanisms of interaction between state law enforcement agencies and the private security sector in the context of the accelerated development of dual-use technologies. The relevance of the study is determined by the fact that the traditional state monopoly on security instruments is gradually losing its exclusive character due to the broad availability of commercial high-tech solutions (AI systems, unmanned platforms, cyber infrastructures). The research examines contemporary formats of public-private partnership, identifies the key barriers to their institutional and technological integration, and analyzes the possibilities of their gradual overcoming. Special emphasis is placed on the transition from minimal forms of cooperation, based mainly on isolated information exchange, to comprehensive, highly integrated smart security systems. The aim of the study is to construct a theoretical model of adaptive risk management arising from the use of private technological solutions in the field of public security. To achieve this aim, methods of systems analysis, comparative legal research, and case studies (based on successful practices of countering identity theft) are applied. The empirical and theoretical foundation of the research consists of foreign sources published in recent years. In the final part, the author's concept of a hybrid security architecture is formulated. The obtained results are of interest to the heads of law enforcement agencies, corporate security practitioners, and specialists involved in the development and updating of regulatory legal acts.*

Keywords: public-private partnership, dual-use technologies, crime prevention, artificial intelligence, cybersecurity, hybrid security.

**Cite This Article:** Ilovača, K. (2026). Mechanisms of Interaction Between Law Enforcement Agencies and Private Security Companies in Crime Prevention. The American Journal of Political Science Law and Criminology, 8(01), 08–15. https://doi.org/10.37547/tajpslc/Volume08Issue01-02.

## 1. Introduction

In the twenty-first century, the configuration of threats to public security is undergoing a qualitative transformation. Criminal activity is becoming increasingly technologically sophisticated, transnational, and covert in its manifestations. Classical hierarchical models of organizing law enforcement agencies (LEA) in many cases fail to adapt to the pace of emergence and evolution of new forms of criminal activity, including cyber fraud, the use of unmanned systems for unlawful purposes, and the appropriation of digital identity. At the same time, private security structures and technological companies (PSC) possess greater institutional flexibility, substantial financial resources, and access to advanced dual-use technologies (DUT) (Dual-Use Technology and U.S. Export Controls. (2025); Rauch et al. (2022). Under these conditions, the task of developing effective mechanisms of cooperation between LEA and PSC acquires critical importance for ensuring national security.

**The aim of the study** is to provide a comprehensive analysis of existing and potential mechanisms for incorporating the resources of the private security sector into state crime prevention strategies. Within this research objective, the following **tasks** are addressed:

— to identify key technological and organizational determinants that either facilitate or hinder the integration of LEA and PSC;

— to analyze the effectiveness of existing forms of interaction using the example of countering property crimes and theft of personal data;

— to develop proposals for the formation of a new adaptive model of regulation and interaction that takes into account the specific risks associated with the use of dual-use technologies.

**The scientific novelty** of the study lies in the interpretation of the interaction between LEA and PSC not as a fixed administrative procedure, but as a dynamically developing ecosystem in which the private sector acts not only as a service provider, but also as a key generator of innovations.

**The author's hypothesis** is that, under conditions of technological turbulence, the optimal model of crime prevention should be based on the principle of shared responsibility: the private sector forms and maintains the technological infrastructure (collection, primary processing, and aggregation of data), while the state concentrates on law enforcement and ethical and legal oversight. The implementation of this approach presupposes the introduction of multi-level regulatory sandboxes that ensure controlled testing and phased integration of innovative solutions.

## 2. Materials and Methods

The methodological basis of the study is a systemic-structural approach that makes it possible to interpret the security provision system as an integral but internally differentiated configuration of interconnected subsystems of the public and private sectors. In the course of preparing the article, a set of general scientific methods was employed: methods of analysis and synthesis were used to reconstruct and integrate existing theoretical approaches; induction and deduction were used to derive general patterns; the method of comparative analysis was applied to compare the regulatory regimes and institutional practices of the United States and EU member states in the field of security and the circulation of dual-use technologies.

The empirical base of the study consists of scholarly monographs, peer-reviewed articles from international journals indexed in Scopus and Web of Science, as well as analytical reports of relevant international organizations and official documents of United States law enforcement agencies, including materials devoted to countering identity theft. The search for sources was carried out through recourse to international full-text and bibliographic databases, as well as to open governmental and departmental registries.

The strategy of bibliographic search was built around the use of English-language keyword queries, such as: interaction between law enforcement and private security, dual-use technology in crime prevention, AI in policing, public-private partnership in security. The chronological scope of the literature selection was limited to the period 2021–2025 in order to ensure the relevance of the empirical material, while fundamental regulatory legal acts were analyzed in their current versions, regardless of their date of initial adoption.

The selection of sources was carried out on the basis of a set of criteria including substantive relevance to the stated topic, the scientific and institutional authority of the publication, and the availability of an empirical base (statistics, case studies, results of pilot projects). Special emphasis was placed on publications devoted to the ethical aspects of the use of artificial intelligence and autonomous systems in the field of security, as well as on issues of export control of dual-use technologies, since these areas in the current configuration of interaction between law enforcement structures and business form the most problematic grey zones of regulation.

## 3. Results

Analysis of the mechanisms of interaction between law enforcement agencies and private security (and related technological) structures shows that contemporary security architecture increasingly relies on the integration of dual-use technologies.

In the classical model, the private sector was perceived by the police primarily as a source of witness testimony or as an object to be protected. At present, according to available data, business structures are transforming into full-fledged and active participants in operational and investigative activities. Indicative in this regard is the example of interagency task forces operating on the model of the LEGIT (Law Enforcement Getting Identity Thieves) type in Florida. Analysis of materials devoted to the activities of this group demonstrates that the successful solving of complex, long-term identity theft schemes is fundamentally impossible without the involvement of the private sector. In this case, described in archival sources, it was precisely the coordinated interaction of sheriffs, state prosecutors, and private financial institutions that made it possible to apprehend the offender. Substantively, the interaction mechanism here is based on distributed data processing: private entities (banking structures, retail) identify and record anomalous transactions and behavior, while law enforcement agencies (LEA) exercise their authoritative coercive and procedural powers.

As for the role of dual-use technologies (DUT), contemporary formats of interaction between LEA and PSC are organically linked to the implementation of dual-use technologies. Studies (Dual-Use Technology and U.S. Export Controls. (2025); Reis et al. (2022) emphasize that commercial developments often outpace their military and police counterparts in terms of maturity and scalability.

Law enforcement agencies are increasingly using algorithmic solutions created by private companies for crime prediction and modeling (Ilovača (2025). Private video surveillance systems integrated with police databases provide the possibility of real-time facial recognition and vehicle license plate identification (Whang (2020). At the same time, such algorithmic infrastructure generates risks of bias, discrimination, and violations of the right to privacy, which necessitates the formation of new, specialized mechanisms for the oversight and audit of such systems.

The commercial drone market demonstrates pervasive implementation. In the context of interaction between LEA and PSC, the key factor is the use of private unmanned platforms for monitoring critical infrastructure, conducting search and rescue operations, and rapid mapping of terrain in the interests of the police (Memon et al. (2024). This reduces the direct burden on the budgets of law enforcement agencies, but at the same time makes strict regulatory governance of airspace use and flight regimes critically important (Raman et al. (2025).

In the field of protecting critical information and digital infrastructure, interaction between the state and the private sector acquires the greatest density. Private companies provide specialized tools and services for penetration testing, vulnerability monitoring, and mitigation of DDoS attacks, while state structures form and maintain the relevant regulatory and institutional framework.

The study of materials devoted to the prevention of fraud in the retail sector demonstrates the effectiveness of local, grounded mechanisms of cooperation. Indicative in this regard is the case of the partnership between the city police and the food chain. The private company, acting as an independent economic entity, on the recommendation of the police modified its business processes (introducing mandatory presentation of identification when paying by check) and returned its video surveillance systems. The result was not only a higher rate of solving the corresponding offenses, but also a pronounced preventive effect. The mechanism here can be described as a chain: consultation from the LEA side → implementation of technical and organizational solutions from the PSC side → subsequent exchange of evidentiary information (video materials and others). Similar instruments described in the Identity Crime Toolkit include organizing events for the secure destruction of documents (Shred-a-Thons) and training personnel in the rules for handling sensitive information. These practices illustrate the use of soft power and prevention-oriented interaction, which reduces the risk of crime commission even before its realization.

Despite the successes indicated, a number of structural constraints and contradictions remain.

– Regulatory lag. Export control systems and special regulatory regimes fail to adapt to the dynamics of the development of intangible technologies such as software, algorithms, and cloud services. This creates regulatory gaps and ambiguity in assessing permissible forms of cross-border interaction.

– Ethics and trust. The use of autonomous systems (LAWS) and AI algorithms generates serious concerns regarding the observance of human rights and the potential for abuse. The lack of proper transparency in the functioning of private algorithmic solutions (the black box effect) complicates their use in criminal proceedings and reduces trust in digital evidence (Whang (2020).

– Compatibility. Complex and inert bureaucratic procedures of public procurement often do not allow law enforcement agencies to promptly integrate innovative products and services offered by the market, which leads to a technological lag of LEA behind the most advanced commercial actors.

Consequently, the conducted analysis shows that dual-use technologies act as a key catalyst for the convergence of LEA and PSC; however, existing models and mechanisms of interaction require profound institutional adjustment and an update of the regulatory framework.

## 4. Discussion

On the basis of the results obtained in the course of the analysis, it can be stated with sufficient certainty that the traditional model of relations between the state and the private sector based on the customer–contractor scheme has in fact lost its relevance and explanatory potential. There arises the need to transition to a fundamentally different configuration of interaction – the Adaptive Hybrid Security Architecture (AHSA) model. This section presents the author's interpretation of how the specified architecture should function in practice; the argumentation is structured and illustrated by means of the corresponding diagrams and tables.

The starting point of the discussion is the recognition of the fundamental inequality in the capabilities of the actors involved. The private sector possesses decision-making speed, flexibility, and access to advanced technologies, whereas the state concentrates in its hands institutional legitimacy and the exclusive right to the use of force.

Table 1 presents a comparative analysis of operational capabilities that substantiates the necessity of symbiosis.

**Table 1:** Comparative analysis of the capabilities of LEA and PSC in the implementation of dual-use technologies (Dual-Use Technology and U.S. Export Controls. (2025); Communication from the Commission to the European Parliament and the Council on Strategic Trade Controls. (2022); Sandhu et al. (2021); Daud et al. (2022)

| Characteristic / Capability | Law enforcement agencies (LEA) | Private security companies (PSC) |
|---|---|---|
| R&D speed (research and development) | Low; constrained by bureaucracy and budget cycles | High; driven by the market and competition) |
| Access to data | Limited to official databases and procedures (warrants) | Broad access to Big Data, IoT sensors, behavioral analytics |
| Legal status | High; authority to arrest, search, use lethal force | Limited; preventive monitoring, citizen's arrest |
| Technology implementation | Reactive; problems with the integration of legacy systems | Proactive; early adopters of AI and drones |
| Responsibility | Public; strict oversight, observance of human rights | Contractual; corporate social responsibility (CSR) |

It is proposed to consider the modern crime prevention system not as a hierarchy but as a concentric system. One of the central mechanisms of interaction identified in the course of the study is the transformation of the format of cooperation from elementary exchange of information arrays to a fusion mode – deep merging and integration of intelligence data. The Consumer Sentinel database considered in the materials can be characterized as an early prototype of this approach; however, the current configuration of threats objectively requires a qualitatively different level, namely a transition to maximally automated processing, correlation and aggregation of such data.

Below, Figure 1 presents the cycle of automated intelligence data fusion.

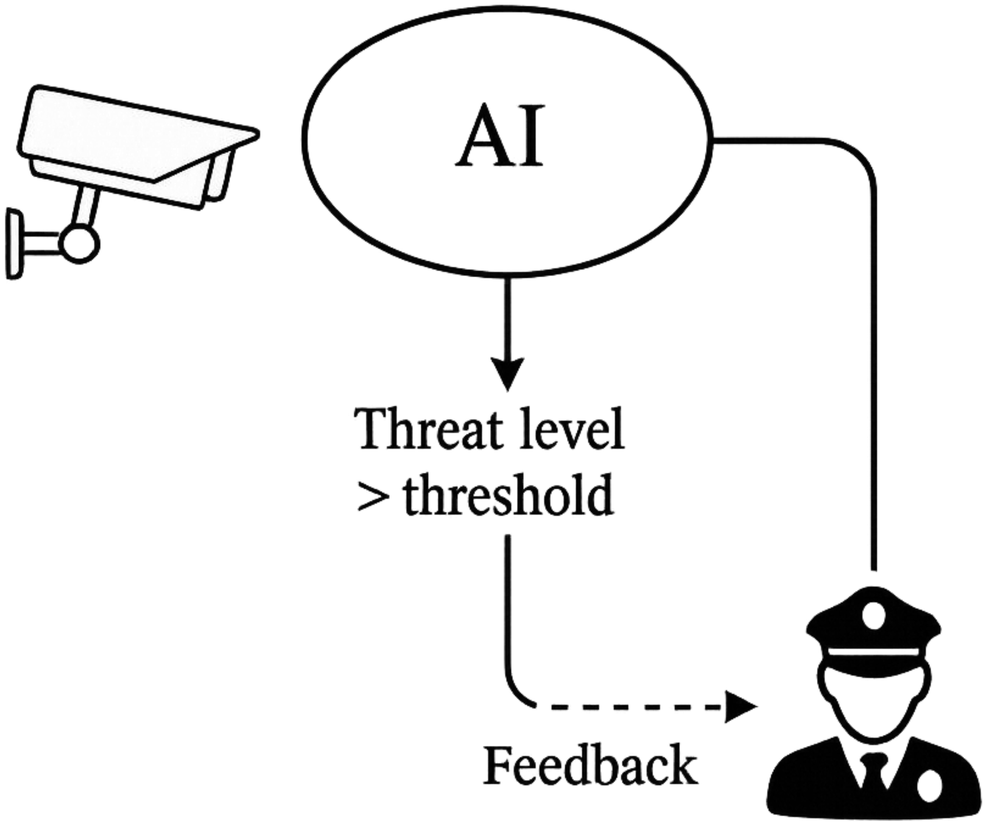

**Figure 1.** Automated intelligence fusion cycle (Reis et al. (2022); Sandhu et al. (2021); Daud et al. (2022)

The figure demonstrates the process whereby an event recorded by a private system (for example, an attempted cyberattack or suspicious behavior in a store) is instantly processed by AI. If the threat level exceeds the threshold value, the signal is transmitted to a police officer. A critically important element here is feedback. The police must inform the private sector about the results so that the system can learn.

The review of scientific and applied literature conducted allows the conclusion that excessively rigid regulatory frameworks constitute a significant obstacle to the deployment and scaling of innovations. As the author's conceptual solution, the introduction of an adaptive governance matrix is proposed, within which technologies are classified not by their typological characteristics, but on the basis of the context of their practical application and the corresponding level of risk.

Table 2 illustrates the proposed regulatory approach.

**Table 2:** Author's matrix of adaptive interaction management (Raman et al. (2025).

| Risk level | Example of technology | Mechanism of interaction | Regulatory requirements |
|---|---|---|---|
| Level 1: Low risk | Video surveillance, basic cyber monitoring, delivery drones. | Open commercial market / Outsourcing. | Standard certification (e.g., Drone Code); Know Your Customer (KYC) principle. |
| Level 2: Medium risk | Predictive AI, biometrics, heavy UAVs. | Licensable partnership / PPP. | Registers of trusted providers; mandatory AI ethics audit; periodic LEA oversight. |
| Level 3: High risk | Lethal autonomous weapons systems (LAWS), offensive cyber weapons. | Strict state monopoly / Special contractors. | Direct operational control by officers; Human-in-the-loop protocols; export ban. |

For the practical implementation of the specified matrix, an institutionalized experimental environment is required within which controlled testing is permissible. Attention has already been drawn to the ethical risks associated with such experiments. A potential mechanism for their managed minimization and the simultaneous stimulation of innovation may be the establishment of regulatory sandboxes.

Below, Figure 2 presents a diagram of the functioning of the regulatory sandbox for dual-use technologies.

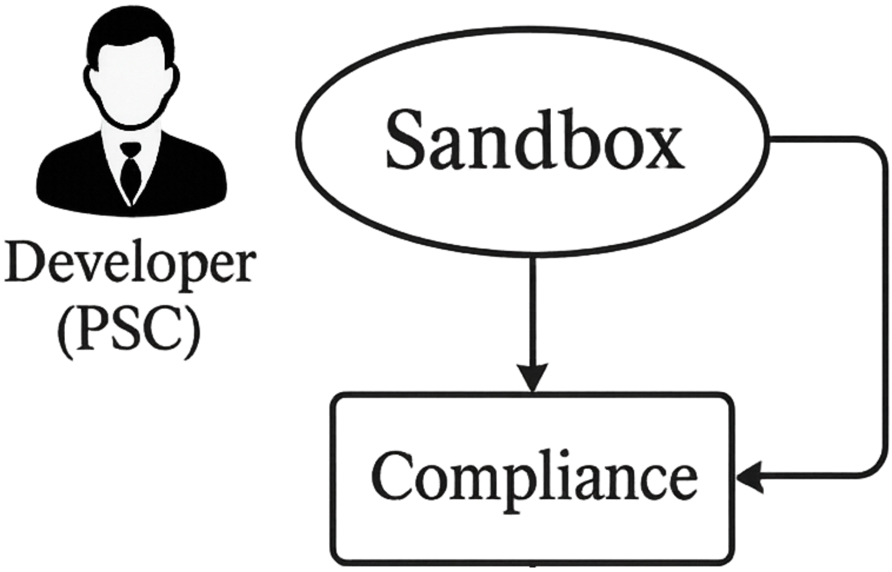

**Figure 2.** Schematic diagram of the functioning of the “Regulatory Sandbox” for dual-use technologies (Daud et al. (2022); Raman et al. (2025).

This scheme illustrates an iterative process. The developer (PSC) proposes a technology (for example, a facial recognition system). Before it reaches the market or the police, it passes through the sandbox, where regulators assess its compliance with legal and ethical standards. Only after the integration of compliance protocols is the product allowed to be put into operation. This makes it possible to maintain a balance between innovation and the protection of citizens' rights.

Ultimately, the analysis conducted demonstrates that the effectiveness of crime prevention is determined not by the number of police resources, but by the quality of the constructed architecture of interaction between key actors. The transition to an adaptive hybrid model based on a multilevel regulatory framework creates for the state an opportunity to institutionally harness the potential of private innovations, while simultaneously reducing the likelihood of losing control over the field of security provision.

## 5. Conclusion

In the course of the research conducted, the mechanisms of interaction between law enforcement agencies and private security companies in the context of the use of dual-use technologies were examined in detail.

It has been shown that such technologies (AI, UAVs, cyber tools) function not only as a set of applied instruments, but also as a system-forming factor that objectively compels inertial state institutions to build partnership relations with the more flexible and technologically advanced private sector.

The analysis of practices for countering identity theft and ensuring public order has demonstrated that the most effective strategies are those based on preventive data exchange and the inclusion of private surveillance systems in a unified public security framework.

The authors hypothesis on the need to transition to a model of shared responsibility has received empirical and conceptual confirmation. The Adaptive Hybrid Security Architecture and the risk-oriented regulatory matrix developed in the study act as concrete instruments for institutionalizing such a transition, making it possible to overcome regulatory rigidity and reduce the gap between the dynamics of technologies and legal regulation.

In this way, the article forms a comprehensive conceptual framework for the modernization of national security strategies. The proposed configurations of interaction (data fusion and regulatory sandboxes) can be directly used in the preparation of regulatory acts governing the circulation of dual-use technologies and the activities of private security organizations.

## References

1. Communication from the Commission to the European Parliament and the Council on Strategic Trade Controls. (2022). European Commission. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0249 (date accessed: 11.11.2025).
2. Daud, S. M. S. M., Yusof, M. Y. P. M., Heo, C. C., Khoo, L. S., Singh, M. K. C., Mahmood, M. S., & Nawawi, H. (2022). Applications of drone in disaster management: A scoping review. Science & Justice, 62(1), 30-42. https://doi.org/10.1016/j.scijus.2021.11.002.
3. Dual-Use Technology and U.S. Export Controls. (2025). Center for a New American Security (CNAS). Retrieved from: https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls (date accessed: 11.11.2025).
4. Ilovača, K. (2025). Implementation Of Dual-Use Technologies in Defense and Public Security. The American Journal of Political Science Law and Criminology, 7(06), 40-48. https://doi.org/10.37547/tajpslc/Volume07Issue06-08.
5. Memon, Q. A., Al Ahmad, M., & Pecht, M. (2024). Quantum Computing: Navigating the Future of Computation, Challenges, and Technological Breakthroughs. Quantum Reports, 6(4), 627-663. https://doi.org/10.3390/quantum6040039.
6. Raman, R., Kowalski, R., Achuthan, K. et al. Navigating artificial general intelligence development: societal, technological, ethical, and brain-inspired pathways. Sci Rep 15, 8443 (2025). https://doi.org/10.1038/s41598-025-92190-7.
7. Rauch, M., & Ansari, S. (2022). Waging war from remote cubicles: How workers cope with technologies that disrupt the meaning and morality of their work. Organization Science, 33(1), 83-104. https://doi.org/10.1287/orsc.2021.1555.

8. Reis, J., Rosado, D. P., Ribeiro, D. F., & Melão, N. (2022). Quintuple Helix Innovation Model for the European Union Defense Industry—An Empirical Research. Sustainability, 14(24), 16499. https://doi.org/10.3390/su142416499.

9. Sandhu, A., & Fussey, P. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. Policing and society, 31(1), 66-81.https://doi.org/10.1080/10439463.2020.1803315 .

10. Whang, C. (2020). Trade and emerging technologies: A comparative analysis of the United States and the European Union dual-use export control regulations. Security and Human Rights, 31, 11-34.