Centre for Defence and Security Strategic Studies &
Interdisciplinary Doctoral School,
"Carol I" National Defence University

DOI: 10.53477/3045-2309-26-15

TWO PARADIGMS OF ALGORITHMIC SECURITY GOVERNANCE: CENTRALISED INTEGRATION AND INTEROPERABLE FRAMEWORKS IN THE USE OF AI FOR STATE SECURITY

Mara-Mihaela MEREANU
Student, Babeș-Bolyai University, Cluj-Napoca, Romania,
Scholar at Shanghai Jiao Tong University, Shanghai, China
E-mail address: mara.mereanu@yahoo.com

Abstract*: Artificial intelligence (AI) plays an increasingly important role in counterterrorism by enabling the rapid processing of large volumes of data and the identification of patterns, anomalous behaviours, and emerging risks. This article examines two paradigms of algorithmic security: the centralised Chinese model and the decentralised, interoperable Israeli model. Adopting a comparative and primarily descriptive approach, the study draws on academic literature, policy documents, and native authors to analyse how AI is embedded within different institutional architectures A brief case study of the 2019 Hong Kong protests examines how predictive technologies were deployed in an urban context officially framed as a matter of security and public order. The analysis shows that the strategic impact of AI depends less on technological sophistication alone and more on governance structures, institutional coordination, and legal frameworks. The study also acknowledges limitations related to restricted data access and the evolving nature of AI-driven security systems.*

Keywords*: Artificial intelligence; counterterrorism; digital surveillance; large language models; national security.*

Introduction

In the past few decades, artificial intelligence (AI) has begun playing an increasingly important role in the field of security and counterterrorism. In the past, data analysis was a slow process that was also fully reliant on human resources, but nowadays the new era of AI technology allows high-speed processing of large quantities of data, thus significantly changing the way both state and non-state actors manage their threats. Through the ability to identify patterns, correlations and atypical behaviours, AI systems provide authorities with additional tools to anticipate risks and implement preventive interventions. In many situations, the response to critical incidents is no longer just reactive, but can be based on predictive analytics, which substantially changes the traditional logic of security management.

By comparing the way in which the states and the violent non-state groups are implementing the use of AI, we can observe a few key elements that are influencing both operational efficiency and strategic stability. Overall, the focus is not confined to equipment and technological infrastructure, or even to the quantity of collected data, but also expands to the way institutions work together, the existing legal framework and coordination mechanisms between security agencies.

In this regard, China represents a particularly relevant case, given how it integrated AI both in a very systematic way and on a multitude of levels. Thus, the state, intelligence agencies, and the technology sector work closely together. Chinese systems combine multi-source data analysis, predictive tools, and digital surveillance, all under the umbrella of centralised governance that aims to prevent, control, and anticipate asymmetric threats.

1. The Chinese model of integrating AI into security and counterterrorism

China is often viewed (Mereanu și Mereanu 2025)as an example when discussing the extensive integration of artificial intelligence into security and counterterrorism. What distinguishes this model is the high degree of coordination between the state, intelligence agencies, and technology companies, which operate within a centralised and well-structured framework. From this perspective, the use of AI in China can be interpreted as part of a broader state-led approach to national security governance rather than as a set of isolated initiatives. Official policy documents present these applications as serving the dual purpose of maintaining internal order and preventing threats, framing them within an integrated vision of risk management.

In practice, the Chinese model involves combining predictive tools, data analysis from various sources, digital surveillance and the use of algorithms capable of identifying behaviours considered atypical or potentially risky. Technology is not treated only as technical support, but as part of the security decision-making mechanism. Thus, AI becomes an integrated element in the process of anticipating and managing threats, both internal and external. (Weber 2025)

In the Chinese security system, the People's Liberation Army (PLA) plays the main role as the armed force of the People's Republic of China. In addition to its traditional duties related to the protection of sovereignty, the PLA has responsibilities in the field of cybersecurity and provides support in the management of internal and external crises. The Ministry of State Security (MSS), on the other hand, functions as the central intelligence and counterintelligence agency. Its activities include monitoring internal and external threats, coordinating anti-terrorist operations, and using digital analysis and Social Media Intelligence (SOCMINT) in situations with an impact on national security. Complementarily, the Ministry of Public Security (MPS) acts as a law enforcement and domestic oversight institution. Although it is not an intelligence agency in the classical sense, the MPS has an important role in combating terrorism, maintaining public order, and monitoring organised crime. In addition, the ministry manages cybersecurity and digital space monitoring, using SOCMINT tools to prevent domestic risks and identify potential threats to social stability. The MPS also manages a vast network of nationwide video surveillance cameras, integrated with local facial recognition systems, which allows it to respond quickly to various security situations. These functions are frequently associated with the "weiwen" (维稳) paradigm – commonly translated as "maintenance of social stability" – which is described in the literature as a central component of China's domestic security (Jun 2010, 29-34).

Thus, by collaborating, the MSS and the MPS practically form the civilian core of China's intelligence system. They work closely with the PLA's military structures, under the coordination of the Communist Party's Central Commission for Political and Legal Affairs, which allows them to maintain a coherent strategy and react quickly in critical situations.

Besides managing security infrastructures, these institutions also tend to function as integration centres for emerging technologies. They coordinate the implementation of predictive systems, advanced behavioural analysis models, and digital surveillance platforms. Given this background, data and algorithms no longer remain just information, thereby functioning as concrete operational tools, capable of supporting the prevention, anticipation, and strategic control of risks. In this context, AI plays a role of efficiency that is difficult to match in other international contexts. A centralised architecture may facilitate the concentration of information flows, reduce institutional fragmentation, and accelerate decision-making processes. In contrast, many Western governance models are characterised by institutional pluralism and divided competences, which can introduce additional procedural constraints. These differences illustrate distinct approaches to integrating AI not only at a technical level but also within broader institutional frameworks.

China has invested significantly in the development and refinement of large language models (LLMs) and advanced machine learning algorithms, integrating them into a coherent multi-source analysis framework. These technologies allow for the simultaneous processing of data from a wide

variety of sources – public information, internal government streams, social media data, and other digital signals – creating a system capable of identifying and preventing terrorist threats, both domestically and internationally. LLMs are not only used for natural language interpretation; they also help uncover complex patterns in social interactions or networks considered at risk of destabilisation, providing authorities with a valuable tool for proactively assessing emerging risks. Furthermore, this analytical infrastructure is reliant on an extended network of international collaboration. China is pooling and integrating data streams with multinational security structures, including those dedicated to counterterrorism. Through the development of advanced tools, authorities are able to generate rapid and robust assessments that allow them to make informed strategic decisions and effectively coordinate operations at a multilateral level. In addition, Beijing seeks to harmonise international standards and best practices, which regulate the anti-terrorism legislative framework, investigative procedures and the protection of critical infrastructures, so that operational efficiency is complementary to respect for fundamental human rights (Mereanu and Mereanu 2025, 27-35).

China's approach is based on an integrated and well-structured governance, in which technology plays a central role in institutional coherence and in strengthening the capacity for rapid response. Large language models (LLMs) are used in an extensive system that includes behavioural analysis, anomaly detection algorithms and predictive digital infrastructures, all directly connected to the state's decision-making processes. Thus, AI does not remain just a technical tool, but becomes an essential structural component in the prevention, monitoring and management of asymmetric threats. (Weber 2025)

Through these mechanisms, China is strengthening its position both operationally and strategically. The combined use of LLMs and multi-source analytics transforms enormous amounts of data into real operational capabilities, facilitating active prevention, reducing uncertainty, and optimising decisions at the international level. This multi-dimensional integration reflects a holistic vision of security, in which emerging technologies and centralised governance complement each other, creating a proactive, coherent, and adaptable prevention model to the complexity of global threats. (Mereanu și Mereanu 2025)

In China's security and counterterrorism strategies, artificial intelligence is widely used in regions with ''ethnically sensitive populations'', such as Xinjiang (The State Council Information Office of the People's Republic of China 2019) and Tibet, but also in other autonomous regions, including Gansu and Qinghai provinces. Here, AI is integrated into a comprehensive surveillance system that combines facial recognition, real-time video monitoring, behavioural analysis, and risk-predicting algorithms.

These tools are described in official discourse as mechanisms for identifying behavioural patterns associated with radicalisation, extremism, or social instability. Proponents argue that such systems can enhance anticipatory risk assessment, assist in the allocation of response resources, and contribute to a more proactive model of security governance. Integrated technologies, including LLMs and multi-source analytics platforms, transform data collected from public sources, internal government streams, and digital communications into concrete operational tools. In this way, surveillance becomes more than a simple response to events; it takes on a proactive and strategic role, enabling the state to identify emerging threats and intervene before they materialize into real risks. (Weber 2025)

Conversely, the urban environment presents specific challenges and opportunities for the application of AI in internal security. Large cities such as Beijing, Shanghai or Chengdu, with high population density and extensive digital connectivity, are integrated into advanced intelligent surveillance systems (Jun 2010). These systems combine facial recognition, real-time video analysis, traffic flow monitoring and online data analysis. In this context, the use of AI is not limited to combating terrorism

itself but also aims to manage the risks related to online radicalisation, disinformation, information manipulation and the rapid mobilisation of social groups.

The 2019 protests in Hong Kong are widely regarded as a significant episode in the evolution of urban security governance. The scale, organisation, and persistence of the demonstrations highlighted potential limitations of predominantly reactive law enforcement models, which rely on physical deployment and post-event intervention. In response, there was an increased emphasis on the development of more technologically integrated systems capable of analysing social, informational, and spatial dynamics in real time to support the anticipation and management of potential escalations.

In the past, social mobilisations relied on community networks built over years, making them difficult to suppress. Today, however, unprecedented connectivity allows people to organise spontaneously – but also gives authorities the tools to track them accurately. As HoFung Hung, a professor at Johns Hopkins University, observed, "it's a double-edged sword": technology can support solidarity and coordination among participants, but it can also be used just as effectively for control and surveillance (Wong 2023). In this context, the Chinese authorities have begun to integrate predictive technologies, multi-source analysis platforms and Social Media Intelligence (SOCMINT) tools. These allow the simultaneous monitoring of online mobilisation, information flows and physical concentrations of people, providing concrete data for planning interventions and preventing the escalation of conflicts. However, these measures also raise numerous concerns at the international level, related to fundamental rights, the transparency of algorithmic decisions and the risk of digital discrimination. From the perspective of the authorities, however, the technologies are seen as preventive tools – intended to ensure regional stability and protection against asymmetric threats – in a vision of security in which prevention always takes precedence over reaction after the incident.

The Hong Kong protests illustrate how contested political events may contribute to shifts in state approaches to urban security governance. Artificial intelligence is no longer just a technical tool – it is becoming an integrative or coordinating mechanism between institutions, helping authorities to react quickly and understand in real time what is happening on the streets or in the digital environment. Advanced language models, behavioural analysis and anomaly detection algorithms work together, directly linked to the state's decision-making processes, transforming enormous volumes of data into concrete actions. In this way, prevention, monitoring and immediate response to threats become operational realities, not just theoretical concepts.

The Chinese case reflects a centralised governance structure in which digital technologies are integrated into state-articulated security strategies. By comparison, countries such as Israel, the United Kingdom, and the United States employ more decentralised institutional arrangements, involving multiple agencies and legal frameworks that regulate the use of surveillance and algorithmic decision-making tools. Looking at these models in parallel, we can see both the advantages and limitations of each approach. They show us how much the institutional structure and legal framework matter when it comes to the effectiveness and legitimacy of using emerging technologies in security and counterterrorism. The use of AI cannot be reduced solely to the idea of technological advancement; it is also reflected in the way the state employs it to prevent crises and maintain social stability.

2. Using artificial intelligence in security and counterterrorism

Israel is a distinct example of advanced integration of AI into national security, combining leading military capabilities, a highly active private technology sector, and an institutional culture focused on rapid innovation and adaptability in the field. In contrast to the Chinese model, which is based on centralisation and hierarchical governance, the Israeli approach focuses on flexible interoperability between intelligence

agencies, the military, and technology companies, with an emphasis on the immediate application of technologies in real-world operational situations.

A key pillar of this ecosystem is Unit 8200, the military intelligence structure of the Israel Defense Forces (IDF), responsible for collecting and analysing SIGINT information and conducting cyber operations. (Farhat 2025) Within the Israeli security architecture, the unit plays a central role in information warfare and in exploiting digital flows relevant to the operational environment (Farhat 2025). In recent years, according to press investigations, Unit 8200 has developed and trained large language models (LLMs) on considerable volumes of Arabic-language data, originating from intercepted communications, text messages and other digital sources, in order to improve analytical capabilities (Heller 2025).

These language models enable accelerated processing of large volumes of raw information, facilitating the identification of recurring patterns, the correlation of data from multiple sources, and the extraction of relevant clues for operational analysis (Heller 2025). Their integration into platforms that combine HUMINT, SIGINT, and other information flows contributes to the formation of a more coherent operational picture and the support of timely decision-making (Farhat 2025). In this sense, artificial intelligence functions as a multiplier of human analytical capacity, optimising the information cycle – from collection and sorting to evaluation and dissemination.

In parallel, the use of analysis algorithms and tools based on machine learning has also expanded in support of military operations, including in the process of identifying and prioritizing targets, as evidenced by discussions on the "Gospel" system and other similar applications (Heller 2025). These developments indicate an increasingly pronounced integration of AI technologies into operational planning and execution processes.

Compared to China, where the integration of artificial intelligence and generative models is subsumed under a highly centralised institutional architecture, Israel operates in a more fragmented framework but characterised by intense interaction between the public and private sectors.

A significant part of the Israeli technological ecosystem is fuelled by former members of Unit 8200, who, after completing their military service, established start-ups with a cyber and AI profile (Heller 2025). This innovation circuit allows for the relatively rapid transfer of solutions developed in the civilian environment to applications relevant to national security, reducing the distance between research and operational implementation.

At the same time, the expansion of the use of artificial intelligence in the security field is accompanied by debates on the ethical and legal implications of these technologies, especially regarding surveillance, data protection and the risk of algorithmic errors in sensitive contexts. While in the Chinese model the legitimacy of AI use is anchored predominantly in the discourse of stability and collective security, in Israel emerging technologies are subject to more visible public and legal scrutiny, even if the security imperative remains a determining factor in the policies adopted.

Overall, the Israeli case illustrates a model of integrating artificial intelligence into the fight against terrorism based on institutional agility, interoperability and accelerated innovation. In parallel, the comparison with the Chinese model highlights two different logics of organising the relationship between state, technology and security: one focused on centralisation and systemic integration, the other on flexibility and the dynamics of the technological ecosystem.

Conclusions

The comparative analysis of China and Israel suggests that artificial intelligence increasingly occupies a structurally significant position within contemporary security governance, extending beyond a merely supportive technological function. AI enhances the capacity to manage vast quantities of data, identify patterns, and assist in making predictions. This transformation shifts

counterterrorism from a primarily reactive approach to one that emphasises anticipation and prevention of attacks.

The previously explored aspects also show that the strategies will not necessarily work better just because technology gets better since the effects of AI depend a lot on the rules and structures of the organisations that use it. China's centralised government model enables the integration of systems, the management of vast populations, and the rapid implementation of predictive and surveillance infrastructures. In contrast, Israel works in a more decentralised but highly interoperable ecosystem where military, intelligence, and private-sector actors work together closely to shape the practical use of AI. These two approaches differ in their configurations, yet they both emphasise a common principle: the strategic advantage of AI arises from the effectiveness of collaboration and governance among institutions, rather than solely from the capabilities of the technology itself.

Nonetheless, the emergence of AI-driven counterterrorism brings forth numerous ethical dilemmas. As predictive analytics and algorithmic systems gain prominence in decision-making, the demand for transparency, accountability, proportionality, and the safeguarding of fundamental rights intensifies. Finding the appropriate balance between security requirements and civil liberties remains a significant consideration in determining the legality and longevity of these models.

In conclusion, artificial intelligence represents more than merely a novel technology; it fundamentally alters how nations perceive and manage security in the digital era. Its role in combating terrorism is set to expand, yet its effectiveness and ethical implications will hinge on the legal frameworks, institutions, and moral principles that regulate its application.

BIBLIOGRAPHY:

Farhat, Jawhar. 2025. *Unit 8200: Israel's Information Warfare Unit.* 03 12. Accessed 02 17, 2026. https://greydynamics.com/unit-8200-israels-information-warfare-unit/

Heller, Mathilda. 2025. "Unit 8200 created AI language learning tool from intercepted Palestinian Arabic comms - report." *The Jerusalem Post.* Accessed 02 12, 2026. https://www.jpost.com/israel-news/article-845128.

Jun, Tang. 2010. "A Study of Risk Administration in Maintenance of Social Stability." *Teaching and Research* 29-34. http://jxyyj.ruc.edu.cn/CN/Y2010/V/I5/29.

Mereanu, Vitia, and Mara Mereanu. 2025. "Strategia Chinei în combaterea terorismului: abordare holistică, cooperare internațională și utilizarea tehnologiilor avansate." *The European Union and the New Dynamic of Global Security* 27-35.

The State Council Information Office of the People's Republic of China. 2019. "Fan kongbu zhuyi he jiduan zhuyi yu renquan baozhang (Xinjiang)." *www.gov.cn.* Accessed 10 18, 2025. https://english.www.gov.cn/archive/white_paper/2019/03/18/content_281476567813306.htm

Wong, Tessa. 2023. *BBC NEWS.* 03 26. Accessed 02 12, 2026. https://www.bbc.com/news/world-asia-64300442