Organization for Security and Co-operation in Europe

HARNESSING NEW TECHNOLOGIES TO ENHANCE CRIME ANALYSIS

SUMMARY PAPER FROM AN EXPERT ROUNDTABLE DISCUSSION AT THE OSCE SECRETARIAT IN VIENNA, AUSTRIA (22-23 OCTOBER 2024)

Disclaimer: This paper summarizes a roundtable discussion held under the Chatham House rule. The views, opinions, and conclusions presented herein reflect a synthesis of the roundtable dialogue and do not necessarily represent the official position of the Organization for the Security and Co-operation in Europe (OSCE) and/or its participating States. This document is intended to capture the essence of the discussion without attribution to specific participants or their affiliations. The OSCE does not endorse or verify the accuracy of individual statements made during the round table. Readers should consider this paper as a reflection of the diverse perspectives shared during the event rather than an authoritative statement on the topics discussed.

OSCE Secretariat
Transnational Threats Department
Strategic Police Matters Unit
Wallnerstrasse 6
1010 Vienna, Austria

E-mail: SPMU@osce.org
www.osce.org/policing

Introduction

New and emerging technologies have transformed almost all aspects of human life. From big data analytics and machine learning algorithms through the Internet-of-Things (IoT), smart sensors and autonomous drones to artificial intelligence (AI) – the current pace of technological innovation is unprecedented. This development has entailed discussions around the benefits and risks associated with the use of new technologies in various professional domains.

In the context of crime and policing, much of the debate has focused on concerns about the threats that such technologies may pose, especially their misuse for criminal purposes. However, the potential of these technologies to revolutionize how law enforcement operates and to enhance both its effectiveness and efficiency, is equally significant.

There is substantial and varied scope for the integration of new and emerging technologies in the work of law enforcement. For example, they can help analyse trends and patterns, monitor security risks and threats, assist in identifying suspects and solving crimes, or streamline various administrative processes and procedures. At the same time, achieving a balance between leveraging technological advancements and safeguarding human rights and fundamental freedoms is an important task that raises ethical, legal and practical questions.

Against this backdrop, the OSCE Secretariat's Transnational Threats Department/Strategic Police Matters Unit (TNTD/SPMU) launched a series of expert roundtable discussions on the use of new and emerging technologies by law enforcement. The discussions aim to identify opportunities for law enforcement to harness new and emerging technologies to support their work, to help formulate policy recommendations, and to explore potential OSCE capacity-building support in this area.

This paper summarizes key points and outcomes from the first round table, which was dedicated to the topic of harnessing new technologies to enhance crime analysis and took place in Vienna, Austria on 22 and 23 October 2024.

Crime analysis in the digital age

The ability to analyse criminal trends and patterns is becoming increasingly important as today's law enforcement agencies seek to address ever more complex security challenges in an environment of limited resources. Crime analysis can significantly contribute to evidence-based and proactive operational and strategic planning, helping to make policing more effective, efficient and responsive.

The rapid evolution of digital technologies has transformed crime analysis and opened up new possibilities. On the one hand, the digitalization of the public sector has enabled law enforcement to more easily access existing data sets and information in various governmental systems and databases. It has made both access to and processing of such data and information much easier and faster. On the other hand, digital technologies

also constantly generate new data about a wide range of human activities. The ever-growing volume and diversity of data offer new opportunities to further enhance crime analysis and make it more reliable, targeted and impactful.

There is a broad consensus that good data analytics can contribute to more effective policing. The ability to analyse massive volumes of data (so-called "big data") in support of tactical, operational or strategic planning and decision-making has thus become an essential part of modern crime analysis. At the same time, collecting, managing and analysing such big data poses a number of practical challenges for law enforcement and also raises important questions in relation to the protection of human rights and fundamental freedoms.

Leveraging artificial intelligence

Machine learning (ML) and artificial intelligence (AI)[1] play a key role in helping law enforcement to leverage the potential of big data to significantly enhance crime analysis. Various applications, especially in the field of data science, have already demonstrated the potential utility of these technologies in the context of law enforcement work. Some important areas where AI is already proving very useful include:

[1] ML is a subset of AI that enables computers to learn and improve from data without being explicitly programmed. It allows machines to automatically learn from past experiences, identify patterns, and make predictions with minimal human intervention. AI is a broader technological field focused on creating computer systems that can mimic human cognitive functions like learning, reasoning, and problem-solving. For simplicity, we will be referring to the broader and inclusive term of AI throughout this summary report.

Automation of manual tasks: AI can automate many manual tasks or processes included in analytical work, such as transcribing hours of audio recordings, and extracting specific keywords or information from a lengthy text. This provides more time for analysts to focus on essential work, including querying the data to dive deeper into a topic, gaining insights and uncovering patterns or trends. However, the validation of automated work still requires human intervention as errors can and will occur.

Data management: AI can help with the management of big data, including categorization and labelling of unstructured or poorly structured data, and cleaning data sets. This can enable analysts to explore data that would be otherwise difficult or impossible to use, for example from legacy databases.

Data analysis: AI is capable of analysing data much faster and on a much larger scale than human analysts. Amid the ever-growing volume of data, using AI to analyse large datasets will become a necessity. This can increase the relevance and quality of analytical products.

Uncovering patterns and trends: AI can be very powerful in uncovering specific patterns or trends in data, especially when provided with clearly articulated and well-defined criteria. At the same time, AI can also help with discovering new correlations in large datasets that human analysts may miss. While correlations do not automatically imply causation and need to be validated, they can offer new avenues for further exploration and generate new insights and understanding.

Image and voice recognition: AI can assist with rapid identification of individuals or objects from vast audio-visual datasets, aiding in suspect tracking, missing person searches or crime scene analysis. They can also help with image classification based on dominant content or objects. For example, AI is already being deployed to analyse satellite imagery to track the cultivation of the crops used for drug production.

Detection and early warning: AI can be used to detect various types of illicit content online, as well as misinformation and deep fakes. It can also be used to highlight signs of new crime trends (e.g., new names for drugs trending online) and provide early warning. Analysts are already utilizing generative AI in order to create scenarios and craft hypotheses in support of ongoing criminal investigations. The utility of AI for these and other purposes is only going to increase as AI technology evolves.

Predictive policing: AI can process vast amounts of both structured and unstructured data, thus providing more powerful and comprehensive analysis to improve predictive models that forecast crime hotspots and trends. As predictive policing is based on the employment of sophisticated statistical methods to gain new insights from various types of historical data, ML and AI can make such analysis more robust. Currently, researchers are exploring whether AI technologies can also be used to eliminate potential inherent bias in data used for predictions and mitigate the risk of producing discriminatory outcomes.

Administrative tasks: AI can assist with numerous administrative tasks. For example, natural language processing tools can transcribe interviews, summarize lengthy documents, translate foreign texts or generate reports. They can also assist with managing schedules and resources or monitoring compliance with procedural requirements. By reducing the administrative burden, these tools not only save time but can also improve accuracy and consistency in routine tasks, thus contributing to better overall operational efficiency.

Training, education and testing: Generative AI can be used for creating entirely new content, including text, images, video or audio. Such "synthetic data" can be useful for training and educating new analysts. It can be also used as an input to train new AI models or to test and validate the functionality of existing systems or tools.

These examples demonstrate the wide range of potential applications and use cases for this technology in the context of crime analysis. However, the utility and effectiveness of AI tools depends heavily on the quality of data and the robustness of their algorithms. In other words, poor quality data will lead to poor results ("garbage in, garbage out"). The effective application of AI tools will also largely rely on the ability of users to understand AI processing of information in order to ensure the transparency of output.

There is also a significant difference between using the capabilities of the existing large language models that have been trained on generic data from the internet and training a brand-new model on more unique and targeted datasets. It is already possible to employ local AI agents that are trained on local or internal data only, which makes their outputs much more accurate and tailored to specific needs or requirements.

Challenges in adopting artificial intelligence

The use of AI to enhance crime analysis also poses specific challenges for law enforcement.

Allocating adequate technical resources

Firstly, training and deploying AI systems requires adequate technical resources. Training sophisticated AI models on internal/local data requires substantial computational power and storage capacities, particularly if restricted to on-premise solutions due to privacy and security concerns. Many law enforcement agencies lack the necessary high-performance computing infrastructure to develop such tools.

This challenge can be overcome by using cloud-based solutions, which can enable law enforcement agencies to access high-performance resources without needing to build and maintain their own infrastructure. In addition, cloud platforms provide advanced AI tools and services, enabling faster model training, real-time data processing, and efficient storage management. In fact, to harness the full potential of AI, using cloud-based systems is necessary.

However, cloud-based solutions come with their own difficulties, in particular regarding privacy and data sovereignty.[2] As law enforcement data often includes sensitive personal or classified information, there are significant concerns about storing such data in a cloud. While there are technical solutions to mitigate potential security risks (e.g., encryption and various access control mechanisms), they may not fully address sovereignty concerns.

States have adopted different approaches to address these concerns. Some jurisdictions have regulations restricting the transfer of certain types of data across borders, making it complicated to use global cloud platforms. Other countries have decided that the benefits offered by global cloud platforms outweigh their privacy and sovereignty concerns. Some countries may decide to build their own national cloud infrastructure specifically for sensitive public sector applications (such as law enforcement, defence or healthcare). Using hybrid solutions that keep sensitive data on-premises while leveraging the cloud for less sensitive tasks, or partnering with trusted cloud providers to build secure and compliant systems, may be another way forward.

Availability and quality of data

The second major challenge relates to the availability and quality of data that would feed into AI models.

Crime analysis often relies on data from a wide range of governmental databases, some of which are outdated legacy systems built without any common standards for data management. Such datasets may contain incomplete, inconsistent, or outdated information as well as various inherent biases, which can all negatively impact the accuracy and reliability of AI models. Additionally, law enforcement agencies frequently rely on siloed databases and systems, making it difficult to integrate and standardize data

[2] Other challenges related to cloud-based solutions may include security risks, vendor lock-in (dependency on one provider), long-term costs, compliance with legal and ethical standards or interoperability with legacy systems.

for effective AI processing. Interoperability of different databases at the national level has been one of the challenges for effective crime analysis for many years, well before the arrival of AI. Merging old and new systems proved to be very difficult in the past and current practice is usually to keep them separated and add an abstraction layer to exploit data from both new and old systems. In this context, AI offers new opportunities as they are particularly suited for working with both structured and unstructured data from various sources. However, this would require moving various datasets to a cloud, which poses its own challenges and concerns as mentioned above.

Interoperability between national and international databases represents an additional challenge when considering how to leverage the potential of AI for crime analysis at the regional or international (global) level. Here, the technical challenges related to joining data across different domains and dimensions are compounded by political and legal challenges related to sovereignty and differences in national legislative frameworks. Nevertheless, it is possible to imagine that in specific crime areas of common interest, some governments could agree to share particular datasets for analytical purposes.

Education and professional training

Another challenge relates to the education and professional training law enforcement practitioners will need to acquire the skills and competencies necessary to effectively leverage the opportunities offered by AI while maintaining meaningful human oversight of their outputs. Training and deploying AI systems will require technical staff with adequate expertise, necessitating law enforcement agencies to either hire new personnel or upskill existing staff.

Integrating AI into analytical work will increase training requirements for analysts, especially in fields such as data science, the functioning and limitations of AI algorithms, statistics and predictive modelling, and human rights and rule of law considerations. Those using AI tools for crime analysis need to have a fundamental understanding of the functioning of AI, its limitations and how to recognize errors in the output including those caused by hallucinations[3] and biases.

In addition, new roles and job profiles may emerge as police support staff are asked to fulfil increasingly technical and specialist functions. Analysts will need to collaborate closely with these new types of staff including data scientists, IT specialists, and other law enforcement officers. In general, crime analyst roles are likely to become more interdisciplinary, blending traditional criminology expertise with data science and IT skills.

Lastly, the professional development of other members of the law enforcement community, including senior managers, will be also essential. Working with big data and AI tools should be integrated into standard police training and education, just like weapons training or driving skills. Critical thinking, human rights awareness, as well as a basic understanding of AI models and their limitations will be particularly important.

[3] AI hallucination is a phenomenon wherein a large language model (LLM)—often a generative AI chatbot or computer vision tool—perceives patterns or objects that are non-existent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate.

Many of the challenges mentioned above can be met with effective change management that addresses the technical and human requirements that such a capability and capacity shift will invariably entail. This will include adapting professional development to the dynamic nature of AI, offering continuous learning to keep pace with technological advancements.

Impact on human rights

The use of AI for crime analysis by law enforcement presents both opportunities and challenges for strengthening human rights-compliant policing. When implemented thoughtfully, AI can improve law enforcement capabilities while respecting, or in some cases even enhancing, individuals' rights. Without careful planning and appropriate governance and safeguards frameworks, however, their use could exacerbate existing inequalities and infringe on fundamental freedoms, posing significant practical and legal challenges.

Enhancing human rights through the use of AI

Looking at the potential positive impact of AI, four areas stand out. First, properly designed AI systems trained on good-quality data can help mitigate human biases in analysis and decision-making by relying on data-driven insights. Empirical evidence has demonstrated the negative impact of human cognitive biases on our ability to interpret the world around us or make decisions, especially in complex situations. Law enforcement practitioners, including crime analysts, are not immune to such biases – especially if tasked with processing and interpreting massive volumes of data and information. Using AI in crime analysis has the potential to reduce the negative impact of human cognitive biases on analytical and decision-making processes. Furthermore, when shortcomings are identified or new rules and regulations introduced, it is much easier to update or improve algorithms to ensure their full compliance than to retrain human analysts.

Secondly, automated processes may increase transparency, accountability and fairness, provided that algorithms are interpretable, well documented and auditable. They can strengthen due process and procedural compliance by reducing arbitrary or disproportionate interventions, enhancing evidence-based decision-making, limiting procedural delays, or identifying patterns of systematic discrimination or shortcomings.

Furthermore, properly designed AI systems with adequate safeguards can enhance the right to privacy. For instance, they can enhance data protection by limiting human access to sensitive information through automated data handling and access logs. They can also enable much more targeted and proportionate retrieval of sensitive personal information, ensuring that only relevant information is accessed for specific policing purposes.

Finally, crime analysts can use AI to detect and analyse misinformation and deep fakes which can help law enforcement to design more effective responses and counter-narratives. This can positively contribute to freedom of speech by fostering a more informed and trustworthy communication

environment and by identifying and mitigating the spread of false or manipulated content. As a result, the use of AI in crime analysis can contribute to preserving the integrity of public debates, protecting individuals from deception, and reducing the harmful effects of disinformation campaigns.

Human rights risks of the use of AI

At the same time, the use of AI for crime analysis undoubtedly has the potential to negatively impact human rights. Indeed, the very same areas that can benefit from the deployment of AI can also face significant risks from these technologies. For instance, while properly designed AI systems trained on good-quality data can help to mitigate some biases, models trained on poor-quality data – such as biased historical data – may perpetuate or even amplify inherent biases, leading to discriminatory outcomes. Profiling and predictive policing based on outputs from biased data may disproportionately target certain communities, for example, leading to their stigmatization or over-policing.

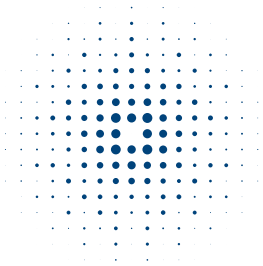
Complex or opaque AI systems may also hinder transparency and accountability by making it difficult to trace, understand or challenge decisions influenced by these technologies. Reliance on flawed outputs from such systems can result in wrongful arrests, detentions, or other infringements of due process rights. Excessively complex or opaque systems also create more opportunities for misuse.

Furthermore, the deployment of AI systems without adequate safeguards can erode privacy and data protection rights. For instance, AI-powered surveillance tools for facial or voice recognition may easily infringe on individuals' right to privacy in the absence of clear safeguards.

Similarly, if implemented without adequate consent or oversight, the large-scale collection of data to train AI models can lead to intrusive monitoring, compromising privacy in both the public and private spaces.

Finally, the use of AI systems for detecting and monitoring misinformation or deep fakes could be easily misused if not deployed with appropriate safeguards and oversight mechanisms. For example, the deployment of such tools to monitor a particular group – for example political opponents or a minority community – could infringe on the freedoms of thought, speech, and assembly, as well as the principle of non-discrimination. Similarly, they may easily be misused for censorship or surveillance of lawful activities.

Ultimately, whether AI will enhance or erode human rights depends on the way these technologies are deployed and used by law enforcement. Careful planning, appropriate governance and adequate safeguards, as well as necessary understanding and expertise within law enforcement are key in this regard. Ensuring that the use of AI does not violate human rights is essential not only for upholding international and national law, but also with regard to maintaining the public trust critical to effective policing. Overreliance on AI tools without clear communication or oversight may undermine public confidence in law enforcement, especially in communities already sceptical of the police.



Conclusion and policy recommendations

The rapid advancement of new and emerging technologies, in particular AI, offers significant opportunities to leverage the potential of "big data" and significantly enhance the relevance and impact of crime analysis. At the same time, the deployment of such technologies poses specific challenges, including for human rights and fundamental freedoms. Many of the challenges can be met with effective change management that addresses the technical and human requirements that such a capability and capacity shift will entail. In this context, OSCE participating States could consider the following policy recommendations.

Deployment of AI in support of crime analysis

- Facilitate regular interdisciplinary dialogue and collaboration between crime analysts, data scientists, legal experts and IT specialists to foster a deeper understanding of the potential benefits and challenges related to the use of AI in crime analysis.

- Develop national regulatory frameworks to guide the development and use of AI systems for law enforcement, ensuring they align with national laws, international agreements and relevant international human rights standards.

- Maintain meaningful human involvement in AI-assisted decisions, ensuring no critical action is taken solely on the basis of AI recommendations. Create channels for public communication about the use of AI in law enforcement, including clear explanations of their purposes, benefits, and safeguards against misuse.

Training and education

- Introduce training for all law enforcement personnel, including senior managers, on the principles, applications, and limitations of AI technologies.

- Develop a dedicated training programme on AI for crime analysts, including subjects such as basics of data science, the functioning and limitations of AI algorithms, statistics and predictive modelling, and the applications of national and international legal and human rights standards.

- Include the development of critical thinking skills in all educational programs for law enforcement personnel, from police cadets to senior management.

Public-private partnership

- Build partnerships between law enforcement agencies and the technology companies that drive AI innovation to co-develop solutions tailored to specific policing needs.

- Support human rights-based AI development by requiring private sector actors to adhere to relevant legal standards in the development of tools for law enforcement, and encouraging the adoption of voluntary schemes for safeguarding human rights in the development and use of AI for crime analysis.

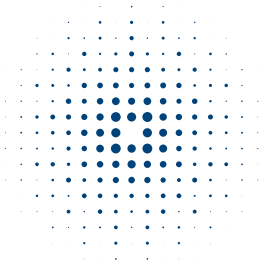
- Partner with trusted cloud providers to develop tailored cloud solutions for law enforcement.
- Facilitate joint investments in AI infrastructure, research, and training to reduce costs and build capacity for deploying cutting-edge technologies.

Accountability and transparency

- Support the development of explainable AI models that are interpretable, with clear audit trails and mechanisms for accountability.
- Require regular risk assessments and audits of AI systems to ensure they operate as intended, and identify and address any unintended consequences.
- Mandate the documentation of algorithms, making their functions and decision-making processes interpretable and accessible to relevant stakeholders, including oversight bodies.
- Consider establishing a dedicated independent oversight body tasked specifically with monitoring the deployment and use of AI technologies in the public sector (including law enforcement).
- Provide accessible mechanisms for individuals to challenge decisions made or influenced by AI systems, ensuring fairness and accountability.

Human rights compliance

- Mandate the use of high-quality datasets to train AI models, and the regular assessment of potential biases in training data, to minimize the risk of perpetuating discriminatory outcomes.
- Ensure all AI systems used by law enforcement are subject to human rights impact assessments before deployment and periodically audit AI models for bias thereafter.
- Prioritize privacy protection by implementing robust data protection measures, including encryption, access controls, and anonymization techniques.
- Develop clear guidelines and operating procedures to ensure that the use of AI systems is proportionate to the intended outcomes and does not unnecessarily infringe on privacy or other fundamental rights.



Further reading

Council of Europe (2024): *HUDERIA - Risk and Impact Assessment of AI Systems*, https://www.coe.int/en/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems

Daniel Bing Andersen, Nina Sunde, Kyle Porter (2025): *Tool induced biases? Misleading data presentation as a biasing source in digital forensic analysis*, Forensic Science International: Digital Investigation, https://doi.org/10.1016/j.fsidi.2025.301881

Europol (2024): *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement*, https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf

INTERPOL and UNICRI (2024): *Toolkit for Responsible AI Innovation in Law Enforcement*, https://unicri.it/Publication/Toolkit-for-Responsible-AI-Innovation-in-Law-Enforcement-UNICRI-INTERPOL

Accountability Principles for Artificial Intelligence, https://ap4ai.eu/

OSCE Organization for Security and Co-operation in Europe