Organization for Security and Co-operation in Europe

2019 Annual Police Experts Meeting

“Artificial Intelligence and Law Enforcement: An Ally or an Adversary”

Opening remarks by OSCE Secretary General

Vienna, 23 September 2019

Excellencies,
Ladies and Gentlemen,
Dear colleagues,

OSCE’s police-related activities are an integral part of our security mandate. Promoting innovative, modern and proactive law enforcement approaches is essential when it comes to effectively addressing transnational threats.

This is precisely the goal of the OSCE Annual Police Expert Meetings. Regrettably, this year I am not able to join you in person due to previous commitments. I am in New York, participating in the UN General Assembly’s High-Level week.

“Artificial Intelligence and Law Enforcement” is a particularly stimulating topic. Many international organizations, including UN agencies, the OECD and the Council of Europe, are already discussing the impact of artificial intelligence on many areas. These include economic growth, transformation of the labour market, privacy concerns and education, just to mention a few.
But, to a large extent, the nexus of artificial intelligence and security is yet to be systematically addressed at the international level.

So the question is: could the OSCE eventually become a platform for enhancing responsible uses of AI, particularly in connection with security?

Ladies and Gentlemen,

We have just initiated this discussion. There is some brainstorming going on in my office, and our Transnational Threats Department is also increasingly engaged in this topic. Dedicating this year’s APEM to AI is another excellent step in the right direction.

But we are still quite far from fully understanding the potential impact of AI on security issues, both in the digital space and the physical world.

Think of the tremendous transformative potential of so-called deep fakes. We are used to understanding digital audio-visual content as a reliable representation of the offline world. Before the eruption of AI, doctored content was in general quite easy to spot. But this reality will be deeply challenged by the proliferation of high quality AI-fabricated audio and video.

In just a few years it will be almost impossible to distinguish facts from noise.

[By the way I can assure this video is genuine! You can ask me when I am back.]

AI algorithms might also lead to the automation of hacking at an unprecedented scale. And, vice versa, AI-enabled software is itself vulnerable to malicious actors
utilizing adversarial attacks. Critical software systems could be severely hit by this sophisticated new form of cyber aggression.

It is hard to imagine the disruptive potential of these tools in the hands of terrorist organizations and criminal networks. Their impact on the well-being of private citizens and the stability of political systems will be unprecedented.

The security challenges of AI-enabled technologies in the physical world will also be particularly acute.

For instance, autonomous drones carrying explosive materials with the ability to recognize a specific, predetermined face will soon be in the toolkit of malicious non-State actors.

On the other hand, the military and law enforcement agencies might be tempted to use autonomous lethal weapons. Should we give machines the decision to put an end to human lives? If you ask me, I don’t think so.

Excellencies,

Besides these and many other unexpected new threats, AI will also offer incredible opportunities for enhancing peace and security. This is particularly true in the domain of law enforcement.

In fact, many law enforcement authorities and agencies have already started to positively apply AI in their work, as we will learn during this event. Just think about AI-enabled algorithms that automatically recognize missing persons or stolen cars. Or advanced crime forecasting tools, such as predictive policing. AI tools can also analyse images from security cameras to identify suspicious
behaviour in prisons or at major events. Of course, care must be taken to ensure that the use of AI by law enforcement respects human rights and is not influenced by unconscious biases.

However, criminal organizations are also quick to adopt new technologies. We have seen it in the past, and AI will be no exception. State-of-the-art AI algorithms are particularly accessible to criminals, since they can often be found online, openly shared by the research community.

Law enforcement and other State institutions will have to keep up and be ready to counter these new forms of crime. International co-operation is essential in this process since the threat transcends national borders. So congratulations and thanks to the Slovak Chairmanship and TNTD’s Strategic Police Matters Unit for organizing such a relevant event!

Dear colleagues,

OSCE’s third dimension of security offers an indispensable angle in this discussion. The right balance between effective policing and protecting human rights and fundamental freedoms must always be a crucial element in both our discussions and practices.

Irresponsible or unethical uses of AI can pose unforeseen risks to our liberties and privacy rights. In addition, algorithmic decision-making has been recently linked to gender and racial bias. Imagine the harmful effect of such flaws on security-related issues.
States and law enforcement agencies should ensure that this technology is used in strict compliance with human rights principles and fundamental freedoms, including regulations related to privacy and non-discrimination.

States should also respect OSCE principles and commitments when using AI in countering threats from criminal activities and when combatting misuse of AI by non-State actors.

So I am particularly pleased that this meeting will dedicate a full session to potential risk factors and ethical and human rights concerns in this area.

Excellencies,

Together with the Slovak Chairmanship, we have put together a very interesting agenda for the next day and a half, with keynote presentations by representatives of international and regional organizations, law enforcement agencies and authorities, academia, and the corporate sector.

Addressing the topic from such a variety of angles will enrich the discussions and enhance our future approaches.

Indeed, OSCE Annual Police Expert Meetings offer more than just an exchange of views, good practices and lessons learned. These meetings aim to produce concrete deliverables.

Let me give you one example: The 2016 meeting focused on intelligence-led policing. A key outcome was the 2017 OSCE Guidebook on intelligence-led policing, which has been translated into at least eight languages. Since then, the
OSCE has been introducing and promoting the intelligence-led policing model in workshops and training events across the OSCE area.

So, dear colleagues, your active participation in this year’s meeting can help determine how the OSCE can best assist its participating States in making effective and responsible use of artificial intelligence in law enforcement.

A “Key Findings and Outcomes” document from this event will provide guidance for future OSCE efforts in this area.

Thank you for your attention and I wish you all a very productive meeting.