EU2019.FI Finland's Presidency of the Council of the European Union

Informal meeting of Justice and Home Affairs Ministers, 18-19 July 2019, Helsinki
Working lunch of Home Affairs Ministers on 18 July 2019

ARTIFICIAL INTELLIGENCE AND LAW ENFORCEMENT

According to the High-Level Expert Group on Artificial Intelligence set up by the European Commission[1], artificial intelligence (AI) can be described as follows:

> *AI systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.*
>
> *As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).*

AI has been high on the agenda of the Council of the European Union since the Digital Summit in September 2017. The European Commission communication, 'Artificial Intelligence for Europe', of 25 April 2018 proposed a European strategy in support of this goal. The Communication also contained a proposal for a coordinated plan for the development of AI in Europe, which was adopted in December 2018.

Brief overview of AI for law enforcement

Information relevant to a particular task is increasingly in danger of getting lost in the ever-swelling tsunami of data. AI could mitigate the problem via intelligent search techniques. For example, intelligent video search could spot an individual fitting a verbal description or a previous photo, or carrying insignia of extremist groups. For an investigator, an intelligent search functionality might unearth similar cases or crime patterns.

Combined with a natural language interface, this technology could form the basis for a digital assistant. Such an assistant could take instructions through a natural

[1] https://ec.europa.eu/digital-single-maret/en/high-level-expert-group-artificial-intelligence

written and spoken discussion, providing a common interface to a variety of applications at the same time, and adapt to the needs of the user. The same technology could power customer service bots that answer questions from citizens. In spoken language mode, the assistant would be helpful to police patrols busy dealing with people involved in incidents. Developing smart digital assistants is vital for making future information overload manageable, but at the same time, we must ensure that the resulting system is transparent to the user.

Another form of intelligent search is analytics. An AI could be trained to detect anomalies or untypical events in applications ranging from autonomous camera surveillance to cyber defence. It could also detect signs of fraud or money laundering from financial data, and in general help to understand criminal phenomena and assess the effectiveness of crime fighting methods. In criminal intelligence, social media analysis could be used to expose links between events, individuals, places, and vehicles. The technology could also play a role in detecting and identifying hybrid threats where a deviation from the norm or normal activity is a significant indicator.

Other security-related AI applications include automated reporting, crime report prioritising, robots and drones for high-threat environments and AI-enriched virtual or mixed reality environments for officer training.

While the need for such applications will increase and diversify, it is necessary to reflect on the necessary framework to ensure the fair, proportionate, and accountable use of these powerful technologies for security purposes.

Direct security threats related to AI

Botnets and machine learning enable hostile actors to conduct massive but tailored cyber attacks and influence operations without significant resources, high-end skills or large numbers of followers. Mass profiling of social media users allows even more sophisticated influence operations. Fake profiles, photos, audio and video are now very easily produced.

A 'deepfake' is a doctored image or video in which a person, either a particular individual or a completely imaginary one, can be made to say or do practically anything: the method is inexpensive to automate and can produce extremely convincing results. Information channels can be swamped with automatically created fake content, eroding trust in media veracity. To counter this, education and media literacy are central. AI tools for detecting influence operations can be developed, but this is difficult and may affect legitimate practices as well, creating an automatic hindrance to free speech. Publicly available services, under independent supervision, could compare news items against a database of known fakes.

The threat of AI-powered cyber attacks will require investment in AI-powered cyber defence. In addition, the cyber security of new AI-enabled products such as driverless cars is a growing concern. Remote identity verification based on facial recognition may open the door to AI-enabled identity theft.

Autonomous, miniature drones could be equipped with facial recognition and used for assassinations or espionage. This could be controlled by setting minimum security standards for dual-use products, and requiring registration for certain types of robots and AI products. A ban on lethal autonomous systems could be considered.

A major challenge is to reinforce transparency in AI-driven technologies. There must be proper control and scrutiny of algorithms to ensure that they are not biased, they yield the correct result and they comply with the applicable legislation.

Indirect security threats and societal challenges related to AI

Deep fakes and other artificial but genuine-looking digital material undermine trust in digital evidence. This may prove extremely harmful for law enforcement, and the development of tools for detecting fake media should be prioritised.

AI development hinges on adequate training data. For instance, the accuracy of facial recognition is dependent on the quality, comprehensiveness, and inclusiveness of the samples it is provided with. Biased, non-representative training data leads to biased performance, which can lead to, for example, discriminatory, mistaken identification. In other applications, the result may be misguided analytics or a misleading digital assistant. Providing lawful access to large and representative datasets for research and training purposes is therefore a necessity, but constitutes a major challenge in the security field.

The mass surveillance that is already a reality in some parts of the world represents a grave privacy issue. It may be possible to automatically collect and process private information such as medical and psychological details from surveillance data.

A society permeated with AI may become too complex to comprehend, which would entail a fundamental lack of transparency. This can be mitigated through system design: for example, a digital assistant should be required to be able to explain its reasoning, and undergo an ethical audit. Guidelines providing accountability rules and defining AI’s role in sensitive decision-making processes are also necessary in order to provide the basis for trustworthy AI.

Other societal challenges posed by AI could include the threat of widespread unemployment and the unrest that would potentially ensue, as well as the increasing dependency on information systems that could lead to increased vulnerability to cyber attacks.[2]

[2] New EU legislation on increased cyber resilience and certification entered into force on 28 June 2019.

Summary

– Information overload is a growing concern in law enforcement work, but a digital assistant capable of intelligent search, and operated by natural language, could at least be part of the solution.

– AI-based analytics provide new insights and tools for crime-fighting.

– AI makes sophisticated cyber attacks and influence operations easy and inexpensive.

– New, genuine-looking fakes may make most digital evidence refutable. It is essential to develop tools for detecting fake and manipulated media.

– Technological robustness and accountability are key: bias in AI training data and a lack of transparency in decision-making processes that rely on AI may make the public distrustful, thereby preventing law enforcement authorities from making full use of AI-powered systems. An ethical audit designed for AI-systems, as well as clear guidelines for the use of AI technologies in police activity, could offer a solution that would address many such concerns.

Questions

In light of the above, delegations are kindly invited to express their views on the following questions:

1. *How do you see the role of AI in relation to law enforcement work?*

2. *Does AI represent a threat or an opportunity and what are the critical factors in its development?*

3. *In the context of law enforcement, should AI be dealt with by Member States individually or should the EU and its agencies/institutions, e.g. Europol, be closely involved in this development? If yes, how?*

4. *In order for the EU as a community to remain internationally competitive as regards AI development, what measures should be taken to maximize the benefit of technologies, knowledge, and training data held by individual bodies, institutions, or Member States?*