EOS Position Paper on

Artificial Intelligence in the Security Domain

Introduction

The importance of Artificial Intelligence (AI) has increasingly been recognized by the European Union (EU) in recent years. In 2017, the European Council acknowledged the urgency of addressing AI and in 2018, EU Member States issued a declaration agreeing to boost Europe's technology and industrial capacity in AI. This was followed by the European Commission's Communication on Artificial Intelligence and by the launch of the European AI Alliance. AI has since been increasingly addressed in EU programmes, including Horizon 2020 as well as the ongoing Horizon Europe and Digital Europe Programme, and has also become the focus of a dedicated European Partnership on AI, Data and Robotics. As highlighted by Commissioner Breton, *"AI is too important a technology for Europe to depend on non-European companies and algorithms. We must therefore organise ourselves to foster the emergence of European alternatives."*

As a disruptive technology, AI has the potential to significantly alter European societies and to provide substantial opportunities and benefits across the entire spectrum of industries and social activities. In addition to driving economic growth and to enhancing Europe's competitiveness on the global markets, AI is key to ensuring Europe's resilience against current and future security challenges. For that purpose, the security aspect is crucial to consider when addressing AI.

Main pillars of AI in the security domain

Three main areas are relevant for AI in the security ecosystem: the use of AI for security, the security of AI systems and algorithms, and the prevention of malicious and criminal use of AI. These three individual pillars may overlap.

AI for security

Artificial Intelligence is not new. The technology has existed and will continue to prosper for a long time, and its potential to bring about opportunities is undeniable. Across different domains, including security, it responds to identified needs of end-users by introducing technological breakthroughs and advances.

The increasingly complex nature of security threats and challenges is driving the digital transformation of the security domain as we know it. Security is heavily reliant on the collection and processing of large amount of data at very high speed. Its ability to do so is critical, even more so than for other domains, as it is a precondition to ensuring appropriate and timely responses to unfolding threats, and hence to ensuring the security and safety of European citizens. This is particularly challenging considering the

rapid development of new technologies and the growing amount of information and data. According to a report published by Europol in partnership with EUROJUST[1], law enforcement agencies are increasingly faced with challenges linked to the use of cryptocurrencies, encryption, inability to identify perpetrators' location, large-scale cyber-attacks, huge data volumes and newly emerging technologies such as IoT and 5G. In response to these challenges, AI – and more specifically data-oriented AI – can bring about innovative and efficient solutions to meet growing security needs.

With AI-enabled solutions, first responders can react rapidly and effectively to a broad range of security challenges, from the protection against cyber-attacks and acts of terrorism to the early detection and response to major anthropogenic or natural hazards such as epidemics.

The potential for improvements in the security domain, through AI, is paramount. Examples include the analysis and interpretation of large amount of data to detect hidden correlations of criminal or hostile activities; the detection of misinformation and illicit content online, including child abuse materials; the protection of public spaces; the enhancement of biometrics and identity techniques by machine learning; the early identification of criminal behaviour and events; the identification of missing people; the recognition and identification of objects; the localisation of terrorist facilities.

Among the different AI applications available for security, facial recognition has emerged as a promising technology to enhance the security of Europe and its citizens. Potential benefits include the protection of populations and sensitive venues – for instance against terrorist attacks, the recognition of deep fakes, and the identification of wanted or missing individuals – including children. For the latter case, facial recognition can be particularly useful as it can identify similarities in faces even as children become adults and can hence assist in finding those who have been missing for years. In India for instance, thousands of missing children have been located after the police started using an experimental facial recognition system software programme. In addition, the technology can also be used by private actors for targeted purposes, such as to secure private sites and assets.

Data-oriented AI therefore provides a wide array of benefits for the security sector. It is not, however, the only type of AI application worth noting. Robotics and cognitive AI are for instance highly relevant to take into account for responding to the capability needs and gaps of the end-users. On the one hand, AI in robotics can enhance robotics capabilities (vision, data integration and understanding, and so on) to perform dedicated tasks or to act in different scenarios. This is important considering that the use of robotics, such as drones, for security has been increasing with time. Robotics provide indeed the advantage of minimising the risks faced by law enforcement officers in the field and hence of enhancing their safety. On the other hand, cognitive AI can support end-users assessing multiple sources of information in real-time and providing hypotheses and conclusions. It can also determine whether an event is real, the origin of the threat, and other indications of a possible attack. By doing so, it can help

[1] Europol and Eurojust (June 2019). Common challenges in combating cybercrime, as identified by Eurojust and Europol. https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF

law enforcement agencies deploy personnel and equipment to the right place at the right time and have the potential ability to defuse hostile situations before they occur.

In light of the significant advantages that AI can bring to enhance the safety and security of citizens, it is therefore crucial for Europe to retain its strategic autonomy in the development of AI systems employed for security purpose.

Security of AI

In addition to the use of AI for security applications, the security and resilience of the AI systems and algorithms themselves is a topic of major importance. This is especially the case when AI is used by critical systems, whose risk of failure would pose a significant threat. AI systems may indeed be compromised by physical or cyber threats – or both. Examples include directly physical interfering with the systems, tampering with datasets used to develop and validate the predictive models, or introducing changes into the algorithms. The different environments where the intelligence is located, namely edge or cloud, should also be considered.

It is therefore important to ensure a high degree of protection of those systems from external cyber-attacks, and to develop European AI systems capable of resisting or countering emerging threats. Considering that human performance is robust to adversarial attacks against AI, a solution may also be to ensure human interaction, especially for high-risk applications.

Techniques such as homomorphic cryptography, multiparty computation and federated learning will also be fundamental to reinforce the security of AI when it comes to data protection. It is fundamental that such protection is implemented using European technologies and solutions, so as to reduce dependence on third countries and strengthen European data sovereignty.

Prevention of malicious use of AI

While the opportunities and benefits brought by AI are undeniable, the technology nevertheless represents a challenge as well. Like any other technology, AI may be used by different actors for diverging purposes, including malicious ones. It is therefore important to carefully consider the threats posed by AI systems when employed by malevolent actors, and to develop solutions to counter them.

The use of AI by criminal, terrorist or state organisations for criminal purposes can have an impact on 3 security domains, namely digital security, physical security, and political security. AI can indeed undermine digital security by launching large-scale cyber-attacks, exploiting human vulnerabilities through impersonation, or manipulating software vulnerabilities via hacking. It can also impair physical security through the manipulation of autonomous systems or the use of drones to carry out for instance terror attacks. When used to target critical infrastructure such as water or energy supply, the technology can even damage the functioning and well-being of a country. Likewise, AI can be maliciously used to

undermine political security through privacy invasion and social manipulation, as well as through fraud and evidence tampering.

Not only have AI-enabled attacks the potential to be effective and targeted, but they are also difficult to attribute. Considering the ongoing progress in AI and the fact that its use may lower the cost of attacks, it is foreseen that the scope of malicious use of AI will increase. This is particularly alarming because malicious trends are growing more advanced and resilient to traditional security measures. In light of these challenges, there is a need to undertake the necessary adaptations of law enforcement measures in order to adequately respond to crimes committed by using such technologies. Any legislative framework must also take into consideration this critical aspect of the malicious use of AI.

Recommendations

EU initiatives

In light of the growing importance of AI and of the disruptive impact it will have on society, it is fundamental for Europe to invest in this technology. From the security perspective, AI will be key to ensuring Europe's resilience against current and future threats and all three pillars highlighted above are critical to take into consideration. Europe should therefore retain its strategic autonomy in the development of AI systems employed for security purposes, reduce non-European supplier dependence, guarantee a high degree of protection of these systems, and adequately respond to crimes committed by using such technologies.

To ensure that these goals are met, research on AI should address the security dimension, including at EU level. It is therefore important that Horizon Europe dedicates sufficient funding to AI in the security domain. In order to guarantee the uptake of the research results, these research activities should also be linked to a capability development and deployment process. Dedicated capability programmes should be launched both at Member States level and at EU level, for instance through the Digital Europe Programme. While the European security industry is already investing significantly in AI, it cannot compete on an equal footing with non-EU players who enjoy strong support from their home countries. If Europe wishes to be in the lead, it is therefore necessary that substantial funding be allocated by EU programmes to AI security topics.

Considering the scope of the security ecosystem, a tri-party collaboration between industry, research community and public authorities is highly encouraged. A structured dialogue among all European security stakeholders is indeed necessary to define AI operational requirements, drive the research and innovation process, and ensure that industry can deliver state-of-the-art solutions compliant with Europe's regulations and ethical values.

The upcoming European Partnership on AI, Data and Robotics is an important step forward in that direction. As the voice of the European security industrial and research community, EOS considers it

imperative to be part of the initiative in order to ensure the adequate representation of the security dimension.

Regulation

EOS supports harmonising legislation at EU level. This is needed to avoid fragmentation of the internal market and diminishment of legal certainty for both providers and users of AI systems. Nevertheless, regulations should be balanced and proportionate, to avoid constraining or hindering technological development or rendering too high the cost of placing AI solutions on the market. With this in mind, EOS believes that the new European Commission Proposal for a Regulation on Artificial Intelligence suggests too harsh requirements that will jeopardise innovation and will slow market uptake of AI. While regulating the use of AI is a requirement to avoid a misuse of the technology, it should not be forgotten that AI systems – even those whose application has been categorised in the European Commission Proposal as high-risk – bring forward tremendous benefits. In some cases, AI can even carry out non-humanly performable functions in highly dangerous environments, such as demining or involvement in nuclear plants and infected areas. In that sense, over regulation should be avoided to ensure that the EU does not lose out on the key competitive advantage that AI can provide to its compagnies and its economy.

As it stands, the approach proposed by the European Commission brings forward a lot of red tape, which risks negatively impacting R&D by slowing down progress and delivery of innovative solutions. It may also negatively affect investments in the AI ecosystem considering the administrative burden and costs it adds onto companies. This is particularly worrisome for SMEs and start-ups, on which the EU often relies for innovation. Specific support for these small entities is therefore required, and while EOS welcomes dedicated measures to address the disadvantages sustained by SMEs and start-ups, the latter are deemed too insufficient and unclear in terms of how they should be practically implemented.

Rather than implementing restrictions on the development of the technology itself, it is the malicious use of AI that should be monitored and regulated. A technology cannot be blamed for its misuse and any technology can in fact be dangerous if used in the wrong context. The users' liability should therefore be taken into consideration seeing as an initial product may be modified based on its application. Nevertheless, regulations implemented should remain balanced and proportionate to avoid the risk of downsizing the demand side of the market.

In this regard, EOS introduces the following recommendations:

- **High-Risk AI systems**
  The Regulation identifies as high-risk a number of instances of AI uses in security and safety related domains such as biometrics, operation of critical infrastructure, law enforcement and border control. The Regulation addresses in particular the risk of infringement of fundamental rights posed by AI systems used by law enforcement and for border control management.

The Regulation justifies the inclusion of those systems into the high-risk category on the ground of possible lack of sufficient accuracy, transparency and explainability. However, this is associated, to different degrees, to the output of any type of decision-aid system. As a matter of fact, human decisions are also frequently affected by lack of accuracy, transparency, and explainability. Moreover, while bias in AI-systems' decisions can be identified and corrected, it is more difficult to do so with human agents.

While mentioning the importance of AI for the security ecosystem, the Regulation de facto ignores the benefits produced in this domain by this technology. For instance, the challenges associated with Hybrid Threats are likely to increase substantially in the years to come. Hostile third countries can leverage digital technologies, direct or indirect links with criminal organisations (including migrant smugglers) and terrorist groups to weaken the social, economic and security fabric of European countries. AI-based solutions will be needed to tackle cyberattacks, ensure the resilience of critical entities, detect synergies with criminal organisations and terrorists, and detect deep fakes. As underlined by the Europol SOCTA 2021 report, the use of deep fakes by criminal organisations is expected to increase, and deep fakes are likely to become widely used in a Hybrid Threats scenario.

EOS believes that a different approach is necessary. High risk should not be defined a priori but based on documented factual evidence in specific use cases, by carefully balancing all different risks faced by citizens, including the risk to their own security. Rather than restraining the use of AI-systems, focus should rather be on judicial or non-judicial safeguards and remedies to possible inaccurate decisions.

- **Requirements on High-Risk systems**

  In EOS' opinion, the Regulation imposes a number of direct or indirect (such as for instance the concept of preventing immaterial harm) constraints on the development and operation of the identified high-risk systems that it will discourage industry to invest in this type of solutions. This approach can have serious consequences for the security of persons and property in the EU.

  Requirements on data sets appear excessively stringent. While having training, validation and testing data sets *"relevant, representative, free of errors and complete"* is the objective that every developer tries to attain, it is in practice an objective extremely difficult to achieve. As per every physical phenomenon, errors can be minimized but never completely eliminated.

  EOS believes that AI compliance processes should be performance-based and adhere to the principle of technological neutrality. Compliance processes need to focus on defining reasonable accuracy thresholds in order to guarantee performances comparable with those displayed by non-AI technological solutions. Where applicable, compliance processes should compare the performance of the AI agent to those of human agents within the same boundary conditions. The error or bias tolerance for the AI systems should be at least as good as that displayed by human agents. Reference to immaterial harm should be eliminated since it is

difficult to assess and could increase the risk of litigations, de facto representing an additional obstacle to the development and adoption of AI solutions. Requirements for free of error data sets should be eliminated to be replaced by an error minimisation approach.

- **Real-time remote biometric identification in publicly accessible spaces**
  The definition of publicly accessible places covers also critical infrastructures such as airports, ports and rail stations. Airports and rail stations represent targets of choice for terrorists. Restricting remote real-time biometric identification in those venues could expose citizens to attacks with deadly consequences.

  EOS believes that real-time and post remote biometric identification should be subject to the data protection measures foreseen by the GDPR regulation and its use should be allowed in critical infrastructures such as airports and rail stations.

- **Sandboxes**
  Sandboxes are a very important instrument to facilitate the development of AI-based solutions, including in the security domain. This is relevant, not only for data availability, but also for having secure environments where to test and assess AI-based or AI-empowered systems, as well as services, data analytics pipelines, or simply algorithms for security.

  EOS believes that implementation of sandboxes should avoid excessive red tape, focus on bringing about viable solutions, while at the same time ensuring minimisation of errors and biases.

September 2021

European Organisation for Security (EOS)
46 avenue des Arts, 1000 Brussels, Belgium | www.eos-eu.com
EOS is registered at the EU Transparency: 32134385519-64