EOS Position Paper on

ARTIFICIAL INTELLIGENCE

As the representative of the European Industrial and Research Security Community, EOS welcomes the European Union's recognition of the strategic role Artificial Intelligence will increasingly play in addressing some of the world's major challenges.

However, EOS urges European institutions to address as a matter of priority the security dimension of Artificial Intelligence.

The importance of AI for the European Union is acknowledged by the European Council's recognition of the urgency of addressing Artificial Intelligence[1] , by the EU Member States declaration[2] agreeing to boost Europe's technology and industrial capacity in AI, by the Commission's Communication[3] on Artificial Intelligence, by the proposal for a Regulation establishing the Digital Europe Programme[4] which intends to respond to the digital transformation challenge focusing also on Artificial Intelligence, and by the June 2018 launch of the European AI Alliance.

However, EOS believes that Artificial Intelligence technologies will become a key factor not only in determining Europe's competitiveness on the global markets but also in ensuring Europe's resilience against current and future security challenges.

The increasing complexity of security challenges is driving the digital transformation of security which rests on the capacity to collect and process large amount of data at very high speed in order to ensure appropriate and timely responses to unfolding threats.

The increasing recourse to Artificial Intelligence in multiple security domains, such as cybersecurity, border management, protection of public spaces and critical infrastructure, requires assurance that the systems will operate in a secure and dependable manner. In fact, it is important for security applications to be able to deploy AI solutions whose outcomes are both explainable and verifiable. In addition, in consideration of the life-critical nature of security decisions, it is important, when defining the operational requirements, to take into account the interactions between humans and AI systems.

Careful consideration should also be given to countering threats posed by AI systems employed by malevolent actors; criminal, terrorist, or state organizations can use AI to conduct cyberattacks; commercial AI-enabled autonomous systems, like drones or mini-robots, could be utilized for illegal activities or to carry out terror acts.

---

1 European Council meeting – Conclusions – 19 October 2017
2 Declaration – Cooperation on Artificial Intelligence – 10 April 2018
3 COM (2018) 237 – Artificial Intelligence for Europe – 25 April 2018
4 COM (2018) 434 – Digital Europe Programme – 6 June 2018

A topic of major importance is the security of AI used by critical systems. AI systems may be compromised by tampering with datasets used to develop and validate the predictive models, or by introducing changes into the algorithms.

It is therefore important for Europe to both retain its strategic autonomy in the development of AI systems employed for security purposes, and to ensure a high degree of protection of these systems from external cyber-attacks.

EOS believes that Horizon Europe needs to take into consideration the security aspects of Artificial Intelligence and that these activities need to be linked to a capability deployment process using both EU security funds (Integrated Border Management Fund and Internal Security Fund) and the Digital Europe Programme.

EOS believes as well that a structured dialogue among all European security stakeholders is necessary to define AI operational requirements, drive the research and innovation process and insure that industry can deliver state-of-the-art solutions compliant with Europe's regulations and ethical values.

European security industry is investing significantly in Artificial Intelligence but in order to compete on an equal footing with non-EU players, which enjoy in this domain strong support from their home countries, it is necessary that substantial funding is allocated by EU programmes to AI security topics.

September 2018