EUROPEAN ORGANISATION FOR SECURITY

EOS Considerations on the ARTIFICIAL INTELLIGENCE WHITE PAPER

11 May 2020

EOS is the voice of the European security industrial and research community who are active in critical domains such as crisis management, cyber, transport and borders. EOS Members, from across 16 European countries, provide security research, solutions, and services to a global market valued at over 400B€, responding to threats that are increasingly cross-border and cross-sectoral, requiring a coordinated European approach across the entire security and safety cycle, from prevention to recovery.

EOS and its members consider Artificial Intelligence (AI) a strategic technology that is having a profound impact on the digital transformation of the security ecosystem. AI-enabled solutions can help first responders to 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. As a matter of fact, non-intentional and malicious hazards are mutually reinforcing and require a unified approach.

EOS welcomes the actions outlined by the European Commission in the White Paper on Artificial Intelligence[1] and would like to present the following considerations:

- A risk-based approach is the most appropriate to reconcile ethical concerns with the need for innovation and the right of citizens to security.
- While EOS generally favours self-assessment compliance mechanisms, it recognises that there can be areas or uses where external assessment procedures are necessary. However, EOS' strong preference is for agile mechanisms that do not introduce unnecessary delays and minimise costs and administrative burdens for industry.
- A very important and often overlooked concern is the use malevolent actors can make of AI technologies. It is essential to develop European AI systems capable of countering these threats and any legislative framework needs to take into consideration this aspect.
- Safety and security represent a technological continuum and this should be taken into consideration when assessing compliance requirements, in order not to unnecessarily stifle innovation.
- Setting up a new public-private-partnership in AI is also a key step for achieving an acceptable degree of European technological strategic autonomy. This is especially true when it comes to safety and security applications.
- **A public private partnership in AI needs to have a dedicated security and safety pillar to properly address operational needs of first responders and to foster strategic autonomy in critical sectors.**

[1] COM (2020) 65 Final – White Paper on Artificial Intelligence – 19 February 2020