Artificial Intelligence: what kind of strategic enabler for EU security and defence?

Report

12 June 2019, Brussels

On 12 June, the EU Institute for Security Studies (EUISS), the Estonian Ministry of Defence and the Permanent Representation of Estonia to the EU, the Ministry of Defence of Finland and the Permanent Representation of Finland to the EU, co-organised a conference on Artificial Intelligence (AI) and EU security and defence. Hosted by the Estonian Permanent Representation to the EU, the event brought together approximately 70 experts from EU institutions, member state governments, academia and industry with the aim of demystifying AI and discussing ways to ensure its responsible use in the defence sector.

A major recurring theme of the conference related to AI and the future of warfare. Panellists agreed that AI is already transforming the way we think about and plan for conflict and deterrence. This is because AI-enabled systems and technologies are already being used by the military and industry. In this regard, there is a need to better communicate to the public the benefits of utilising AI in security and defence. The shock factor of the 'killer robots' label masks the fact that AI is already being used to assist EU institutions and member states in areas such as crime fighting, piracy, search and rescue and border management. For example, AI-enabled systems support human and satellite analysis by extracting information from satellite images, improving image clarity and sifting through huge amounts of image data.

Most panellists agreed that AI will transform warfare especially in the areas of targeting, surveillance, communications and logistics. Countries such as the US and China are likely to integrate AI into defence systems for the foreseeable future, but it was acknowledged that AI-enabled technologies could also in time be used by terrorist organisations and criminal groups. It is for such reasons that Europe cannot afford to fall behind the AI technology curve. In this respect, the audience acknowledged the European Commission's AI Strategy and the decision to invest €20 billion in AI over the next two years and possibly beyond. The discussions over the next Multi-annual Financial Framework and steps towards a 'European Defence Union' can help further define the EU's approach to AI and security and defence.

Working towards a European approach is vital not only from an ethical point of view, but also because it could lead to technological economies of scale in Europe and enhance the interoperability of Europe's armed forces. Indeed, the development of AI-enabled technologies in Europe poses a challenge with regard to interoperability because EU member states and NATO allies have different approaches to AI and they are at different stages of thinking about how AI might affect their security and defence. Nevertheless, AI presents an opportunity for Europe's armed forces because it

potentially allows for greater situational awareness, surveillance capacities, enhanced cyber defence, efficient logistics and supply chains and it may even reduce loss of life and financial costs.

In this respect, investments under the European Defence Fund (EDF) could be geared to AI-supported communication systems, cyber defence, logistics and more. AI can therefore be seen as an industrial and technological opportunity for Europe but a number of challenges need tackling. The reality today is that government institutions and defence ministries do not necessarily have the skills needed to use or apply AI-enabled systems. While the use of AI is an effective way of offsetting personnel shortages in Europe's armed forces, most young graduates or skilled computer technicians, engineers and scientists are more likely to want to apply their skills in the civilian domain.

Ethical issues were also raised during the conference. Panellists recognised that although AI could bring benefits to EU security and defence, humans should remain in the loop in order to ensure responsible use and accountability. It is still the case today that humans are required to analyse data that is collected by AI-enabled technologies and this means that individuals using such technologies need to be sufficiently trained in AI-enabled technologies, software and systems. The need to develop AI skills is also a reason why many speakers placed an emphasis on the need for EU institutions and agencies to work closer together on AI in security and defence.

In this respect, guidelines for trustworthy AI have already been put forward with regard to civilian applications and many of the guidelines can also be applied to the military domain. The European External Action Service has assembled a Global Tech panel and the European Defence Agency is preparing a mapping of relevant AI technology domains. The European Parliament is of the belief trust within society on AI is imperative.

An important part of the EU's approach to AI in security and defence is the need to further study the relationship between the private and public sectors developing AI-enabled systems. Private companies are innovating at a rapid pace and this may confer on them a dominant position when it comes to designing, developing and deploying AI-enabled systems. 'Silicon valley' type firms are managing vast amounts of data and there is a need to ensure that they follow ethical standards. The EU's General Data Protection Regulation is just one tool that can be used to ensure that new technologies adhere to ethical and regulatory standards.

Even though Europeans are keen to develop AI-enabled systems in a responsible manner, however, non-European developers may not necessarily encode ethical safeguards in their own systems. This is especially true given the lack of international agreements and legal frameworks. There is research that shows that there are significant differences in the way AI systems are programmed in different regions and countries. How AI-enabled computer and weapons systems are encoded is a key challenge. Algorithms tend to reflect the moral bias and assumptions of programmers. In addition to ensuring that AI reflects European values and existing international law, a deeper reflection on what AI proliferation (to state and non-state actors) may look like is critical. Finally, while AI can be an industrial and technological opportunity for Europe there is a clear need to study what effect the importation of foreign AI-enabled systems could have on the European market and in terms of the maintenance of ethical AI systems.