THE EU, NATO AND ARTIFICIAL INTELLIGENCE

New possibilities for cooperation?

Report

On 14 November 2019, the EU Institute for Security Studies (EUISS) and the Finnish Presidency of the Council of the EU organised a conference focused on possible future cooperation between the European Union (EU) and the North Atlantic Treaty Organisation (NATO) on Artificial Intelligence (AI). Hosted by the Finnish Permanent Representation to the EU, the event allowed participants to exchange views on the state of play on AI and defence, the challenges posed by AI for the two organisations, as well as the parameters of potential EU-NATO cooperation. The conference brought together key representatives from the EU institutions and NATO, member states, think tanks and academic institutions.

UNDERSTANDING ARTIFICIAL INTELLIGENCE

At the event it was agreed that AI should be conceptualised as a key part of a broader nexus of emerging disruptive technologies, alongside big data, quantum computing and autonomous systems. While its exact impact remains unclear, there was consensus that AI-enabled systems would inevitably transform defence across the board. AI could enhance data management and situational awareness capacities, leading to cost-savings, improved feedback control systems and decision-making, new operational concepts and greater freedom of action. On the battlefield, AI could function as an enabler across all future platforms and capabilities, with main areas of application including C2, ISR, training and logistics. As such, it would become a key factor in interoperability. AI could also change the organisational structure of military institutions in numerous – and often unpredictable – ways. In strategic terms, it could potentially lead to a reduction of the level of kinetic violence in conflict, altering the military's role in controlling the battlefield.

Participants also discussed the challenges stemming from AI's nature as a dual-use technology developed primarily by the private sector. Since national defence was not the main driver of the development of AI, there were concerns about the erosion of the military's ability to maintain its technological edge and ensure the uptake of its concerns by civilian developers. Another challenge related to the risks of proliferation of AI technologies to non-state actors, particularly in conjunction with cyber. Furthermore, it was pointed out that, notwithstanding its desire for technological sovereignty, Europe was lagging far behind the US and China in terms of investment in AI and digitalisation. Participants also noted the heavy Chinese and Russian investments in autonomous systems, which is fuelling an unease about a potential new 'Revolution in Military Affairs' and a subsequent 'AI arms race'.

EU-NATO COOPERATION SO FAR

With regard to EU-NATO cooperation, the progress achieved in several domains was noted, especially in the context of the Joint Declarations. Countering hybrid threats, in particular, was a key area of common efforts, as concretely embodied by the European Centre of Excellence for Countering Hybrid Threats. In this respect, a natural division of labour had emerged, with NATO leading in the 'warfare' aspects of hybrid threats and the EU in the less military-intensive ones. It was asked whether an expansion of this sort of cooperation on AI was possible. Here, it was acknowledged that both the EU and NATO were just beginning to grapple with the issue of AI in defence, whereas

Russia and China had already started thinking strategically and had articulated ambitions for leadership and self-sufficiency in AI.

The EU is mainly active in the civilian dimension of AI and had yet to orientate itself strategically, although a recent food for thought paper on digitalisation and artificial intelligence in defence drawn up by Finland, Estonia, France, Germany and the Netherlands represented a first step in that direction. From its side, NATO had still not developed a military AI strategy of its own, although it was putting increasing effort into AI. In this context, the EU and NATO had nevertheless already taken their first steps in cooperation in AI with the NATO Science and Technology Organisation participating in EU-funded projects, while Sweden and Finland have participated in NATO projects at the working level.

However, the conference also addressed specific challenges to cooperation. It was pointed out that the two organisations occasionally held diverging perspectives on particular issues, such as Lethal Autonomous Weapon Systems (LAWS) or the appropriate balance between laissez-faire and dirigiste approaches to defence industrial and technological matters. The fact that not every EU member state had published their positions on AI yet, while the US AI military strategy does not even mention NATO, did little to bridge these divergent viewpoints. It was also highlighted that despite any possible need for cooperation on AI, the respective mandates and autonomy of each organisation should be respected.

NEXT STEPS FOR EU-NATO COOPERATION

A shared view at the event was that moving EU-NATO cooperation forward was essential. As in the cyber domain, the two organisations could play complementary roles, drawing on their respective strengths and instruments, with the EU leading in dual-use and NATO in military standards. The importance of shared values and outlooks was also highlighted on several occasions. The two organisations held similar perspectives on fundamental issues, including the unknown qualities of AI in defence, the need for technological partnership between democracies, an AI arms control regime and strong links between government and industry. In addition, cooperation required a shared understanding of AI. Creating a common vocabulary was key in this respect, an area that the European Defence Agency (EDA) was already working. It was also noted that inter-institutional cooperation would not be fully effective until each organisation developed an internally coherent outlook, with clearly defined goals, threat perceptions and a goal-driven approach to AI.

On this basis, a number of specific areas for increased EU-NATO cooperation were discussed during the discussion. It was proposed that further steps were taken to implement the Joint Declarations, including possibly by establishing an 'AI Centre of Excellence'. Another proposal concerned adding an AI research dimension to the Declarations, although a different view contended that AI would nonetheless automatically and incrementally feature in EU-NATO cooperation given its cross-cutting nature. The need for a common EU-NATO data-management and data-sharing framework was also proposed, in light of the importance of data pools for the performance of AI algorithms. Although much remained to be done in that area, data labelling was identified as a good starting point.

Another point raised on several occasions was the importance of interoperability. Here, it was argued, AI had the potential to either increase or decrease existing gaps. Militaries could mitigate AI interoperability gaps through exercises and common training, such as through the Cyber Education Platform, or by developing niche capabilities, especially by utilising EU initiatives such as Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF). Some participants argued that divergences were nevertheless inevitable and that, consequently, countries with low or no AI capabilities should be able to trust the technologies of those with more advanced technologies. This, in turn, required a common framework for certification and evaluation procedures, as well as standardised interfaces and modular system architectures that would combine closed/'national' and open/'shared' components.

The conference also highlighted the crucial role of private-public partnerships in bridging the gap between research and capability development and ensuring that defence concerns were taken into account by civilian developers. Government support to science and technology, but also to industry was essential in this regard, particularly

in relation to testing, certification and prototyping. The EU was well suited to provide such support through the EDA and EDF and by developing relevant standards, regulations and processes. Furthermore, the need to reduce dependence on global value chains for key AI components and technologies was underlined. In addition, militaries would have to become more agile in defence planning and procurement in order to be able to catch up with and access new private sector-led technologies, but – equally importantly – also to integrate and adapt them.

Another topic of discussion during the conference concerned the importance of regulating AI and preventing its uncontrollable proliferation, in line with the values underpinning both organisations. In reference to LAWS, there was agreement that the application of existing international law should be explored before considering the development of new instruments. Opinions diverged, however, regarding the appropriate balance between strategic and ethical considerations, with some participants pointing out that other global powers largely ignored the latter. Relatedly, the point was also made that AI ethics and regulations had limited effect in any case, as long as the technology itself was developed elsewhere. Therefore, it was imperative that Europe boosted investment in AI capabilities, in line with the new Commission's pledge on digitalisation. In this context, member states would have to be prepared to take financial risks, considering that not all investments would pay off.