AI for Defence

Edward Hunter Christie

Remarks delivered at the Aspen Central Europe Annual Conference held in Prague, Czech Republic

2 December 2021

To cite this speech (APA):
Christie, E. H. (2021, December 2). *AI for Defence* [Speech transcript]. AI Policy Blog.

I'm going to talk about Artificial Intelligence and Defence, in particular based on the experiences I had in that space while working as a NATO official and later as a consultant to NATO. The views I express are my own.

Artificial Intelligence in its current wave is primarily centred on Machine Learning, including Deep Learning.

One way of understanding Machine Learning is that it consists of automated statistical learning algorithms that are trained on large datasets, such that they become very effective at correctly recognising patterns and making predictions when encountering new real-world data.

And the data in question can be of any type: numbers, text, audio, images, video – if it can be digitised, it can be used. And that covers a full range of what is needed.

Since a few years, Machine Learning algorithms perform better than humans on a quite broad range of pattern recognition and prediction tasks. And with appropriate eyes and ears on robotic systems – meaning sensors – we're looking at a world of intelligent connected devices – autonomous devices – capable of determining their own courses of action to solve particular mission objectives. This may occur with the devices acting alone, or in collaboration with other robotic systems, or in human-machine teams. And that may be in the cyber domain, or in any of the physical domains of military operations – Air, Land, Sea, or Space.

That is the direction of travel and the promise of AI – provided we invest well, have the right policies in place, and make efforts to stay ahead of potential adversaries and competitors.

At NATO, the priority has been to develop policy according to two main pillars: Dynamic Adoption and Responsible Use.

Adoption refers to investments and new mechanisms to ensure a more rapid throughput of the best available technologies into the world of military capability development.

Responsible use refers to principles that Allied governments have committed to, to ensure that ethical and legal considerations are integrated and to guide the development of new capabilities, while also providing a baseline level of commitment on the international stage and for engagements with non-Allies.

The principles are:

A. Lawfulness
B. Responsibility and Accountability
C. Explainability and Traceability
D. Reliability
E. Governability
F. Bias Mitigation

A few comments on some of the principles.

The principle of Responsibility and Accountability refers to the notion that military users shall remain responsible and accountable, including in the legal sense, and in line with the relevant chains of command. It will not be the case that the AI capabilities themselves are deemed responsible, or that nothing or nobody is deemed responsible. Responsibility and Accountability relates to human decision-makers, as is the case with any other military capabilities and use of military capabilities.

The principle of Reliability includes commitments towards the safety, security, and robustness of AI capabilities. This includes ensuring that AI capabilities are robust to data environments that occur under real-life operating conditions. We can't have systems that are completely thrown off course because colours and luminosity have changed because the weather has changed. The principle also addresses AI being secure from deliberate attacks – spoofing, data poisoning, or model extraction attacks, for example.

The principle of Governability includes the ability to disengage or deactivate a system if that system demonstrates unintended behaviour. This ability may be built in based on the possibility for human intervention, but also through the possibility of distinct control software which could detect unintended behaviour and respond faster than a human supervisor could hope to achieve.

What is the work that lies ahead?

With the adoption by Allied governments of the first NATO AI Strategy in October 2021, the Alliance now has the essential policy building blocks in place, and so moving forward we're looking at very concrete steps to continue the development and integration of new capabilities and to pursue the practical implementation of the Principles of Responsible Use.

The Alliance's Science & Technology expert communities, its capability development communities, its standardisation communities, its military end user communities, all will play key roles in driving the work forward.

Test centres will play an important role in Testing, Experimentation, Verification, and Validation of what capabilities can do – and of how they stack up as compared to the Principles of Responsible Use.

Efforts to accelerate technological development will be crucial – requiring greater state investments in defence R&D, as well as new and streamlined pathways to collaborate with leading industry and academic players.

Through ongoing work on common NATO standards, interoperability will remain central to Allied efforts.

And so it is my hope that Allies in Central Europe, notably the Czech Republic, will find new ways of contributing to this major area of work.

This is an exciting time for technologically gifted innovators and entrepreneurs who want to contribute to the defence and security of Europe and of the Atlantic Alliance.

Thank you.