NATO Foundation
Defense College

Fondazione
Compagnia
di San Paolo

The Alliance in the loop: NATO and Artificial Intelligence

Federico Berger

Junior Fellow, NDCF

NATO Defense College Foundation Paper

Executive Summary

After a rollercoaster of great successes and setbacks, Artificial Intelligence (AI) seems to be living a new golden age, especially in the defense sector. In a nutshell, Artificial Intelligence is the ability of machines to simulate and mimic the problem-solving and decision-making processes of human brain related to specific tasks with a certain degree of autonomy, doing so by processing a large amount of information at high speed and leveraging on software capabilities, algorithms and deep neural networks, and an ever-increasing volume of data (the so-called "AI triad").

Although AI is already employed by NATO for Information and Decision Support and Robotic Autonomous Systems (RAS), its R&D process and potential applications seem far from over, as testified by the NATO 2030 initiative and the last NATO Summit in Brussels.

But with opportunities, there come challenges. First, the Alliance needs to work effectively with all its members to establish what technologies better fit with the operational needs in order to avoid a waste of investments.

Second, NATO should analyse the state-of-the-art in all Allied countries, coming out with a deep understanding of what is the competitive advantage of the single nation and then coordinating the development of capabilities through cooperation within the NATO umbrella.

Third, NATO should take into account the existence of dedicated national agencies in some of its countries, in order to avoid the duplication of structures and resources and sustain less-developed realities.

Fourth, the Alliance should retain its privileged position among Allies, helping with the creation of common R&D and use standards and procedures through open international dialogue. Only shared agreements, involving the private sector, the NGOs, the academia, and tech firms, guarantee a balanced and proportionate handling of EDTs.

1. History and Definition

Historical overview

Since Alan Turing (widely considered the father of the subject matter) came out in 1950 with probably his most famous article "Computing Machinery and Intelligence" and the even more iconic "Imitation Game", Artificial Intelligence (AI) has experienced a rollercoaster of successful periods and years of scepticism and doubts.

Once the initial doubts due to the costs and physical limits of machines were overcome, from the late '50s to the middle of the '70s the AI sector flourished, especially thanks to dedicated research programs of different entities funded by government agencies (like the US DoD's Defense Advanced Research Projects Agency or DARPA) with evident concerns from the defense sector. The years of Gordon Moore's Law (196), were dominated by a widespread conviction among the scientific community that an Artificial General Intelligence (AGI) was achievable: thanks to the ramping technological advancements, machines would not just be able to solve complex tasks of humans, but rather to replicate (if not surpass) human intelligence.

Enthusiasms were soon curbed by the very first so-called "AI winter", a specific period of time corresponding to the late '70s and early '80s dominated by scientific pessimism towards AI systems and a reduction of funds for research. Scientists had to deal with the lack of computational power to do anything substantial: computers were not able to process information quickly or to store consistent amounts of data properly. In addition, results were not communicated effectively and were difficult to be understood if not by expert computer scientists.

But during the 1980s, the popularisation of on the one hand "machine learning" techniques and their subfield called "deep learning" (able to make accurate predictions based on repeated operations and experience), on the other "expert systems" (mimicking the decision-making process of human experts) gave new life to the sector. These technologies defrosted the AI winter and attracted a new wave of funds: while expert systems were already used in the private sector, as an example the Japanese government heavily funded research in the field through its Fifth Generation Computer Project or FGCP, with the intent of modernizing computer processing and implementing logic programming.

Although a large part of the goals was not met, the second wave of AI fervour may have ignited and inspired the new generation of researchers in the 1990s and the 2000s. Despite the fact that a part of the scientific community believes that an AGI will soon come (due to flashy technological innovations), the focus on neural networks and expert systems is driving the R&D compartments towards the so-called “narrow AI”, systems able to handle a singular or limited task. Because of their sharp and practical adoption, this kind of systems are gaining particular attention from the private sector and the industry, as well as the whole practitioners’ community is urged to develop a more measured, realistic view of AI's capability. Overall, the sector is supposed to have an economic impact between 1.5 and 3 USD trillion between 2016 and 2026.

While nowadays’ software and computation capabilities, machine learning techniques, and data availability allow machines to perform complex tasks like driving unmanned vehicles, identifying human faces and animals, translating text in every language, or spotting tumours, there is still wide room for growth. As Edward Grefenstette declared to the BBC, “One of the biggest challenges is to develop methods that are much more efficient in terms of the data and compute power required to learn to solve a problem well”, rather than develop systems that can solve all problems. Otherwise, the risk is to fall once again into an AI winter.

A definition for the defense sector

Drawing from current trends in the market (which remains the driving force of technological development) and research, and building on the findings of the NATO Foundation’s conference “Game Changers 2020” – taken from the interventions of Peter Nielsen (Aalborg University), Andrea Gilli (NATO Defense College), Roberto Manca (Italian Air Force), and Stephan Breunessaux (Airbus), a definition of Artificial Intelligence as comprehensive and operative as possible emerges.

In a nutshell, Artificial Intelligence is the ability of machines to simulate and mimic the problem-solving and decision-making processes of human brain related to specific tasks with a certain degree of autonomy, doing so by processing a large amount of information at high speed and leveraging on software capabilities, algorithms and deep neural networks, and an ever-increasing volume of data (the so-called “AI triad”).

With these features in mind, it is observable that AI already finds its room for application in the defense sector for:

- Intelligence Surveillance Reconaissance – ISR (e.g. object tracking, detection, and identification, or sensor data fusion);

- Logistics (e.g. vehicles or aircrafts maintenance);
- Cyber and Electronic Warfare (for both offensive and defensive purposes);
- InfoOps (e.g. deepfakes creation or detection);
- Command and Control (for decision-making support).

A further point, linked to AI, is related to automation in the battlefields, with new technologies like task-based agents, loyal wingman, swarming, and autonomous target recognition and engagement emerging.

The application of AI in the defense sector raise at least two main issues related to automation (the self-governing technical procedures), autonomy (the level of independence to take a decision), and control (the degree of human's oversight over the process).

From an operational point of view, these new technologies on the one hand may lead to an arm race among nations to exploit new advantages and gains with implications for deterrence, on the other may increase speed and magnitude of the escalation of violence on the ground due to increasing automation (since machines are not able to understand the context).

From a decision-making perspective, the technological challenge of AI's implementation in the "decision-centric warfare" requires processual and cultural changes. As leaders will have to think in a more probabilistic mindset, they will need strategic-level education to work as the "man in the loop" in an interactive environment with machines, in order to achieve better solutions than either would arrive at alone.

2. NATO's approach towards AI

As suggested by the RAND think tank and quoted by the NATO Review, the North Atlantic Treaty Organization groups AI into three main types of applications:

1. Enterprise AI, such as AI-enabled financial and personnel management systems (where the implications of technical failures are low in terms of danger and mortality);
2. Operational AI, like control software of stationary systems or unmanned vehicles (with severe implications in case of failure);

3. Mission Support AI, including diverse applications like logistics and maintenance, or intelligence-related application (an intermediate category in terms of environment control and failure implications).

The 2019 Report drafted by the Science and Technology Committee (STC) for the NATO Parliamentary Assembly clearly mentions two key areas of opportunities for the Alliance in the enhanced adoption of AI: information and decision support, and robotic autonomous systems.

Information and decision support

While political and military leaders have always had to deal with the "fog of war", today's complex world urges faster, sharper decision-making to keep the pace with the speed of change. In military terms, AI can sensibly boost the rhythm of analysis and action in different ways, namely improving the reaction times of defensive systems against hypersonic weapons, cyberattacks, or directed energy weapons, delivering actionable information faster, helping in detecting hostile actions carried out by adversaries in cyberspace.

The adoption of AI brings benefits to the quality of the decision-making indeed. The data-rich Information Age is posing serious challenges to human resources, and AI-powered solutions provide better visualization of data (enabling more effective interpretations), automatically extract objects of interest from data feeds for follow-up actions, extract highly-significant "weak signals" for intelligence operators, suggest likely options and possible effects of different choices, analyse adversarial behaviour through foreknowledge.

Robotic Autonomous Systems (RACs)

The growing application of AI in the defense sector is going hand-in-hand with the rapid proliferation of RACs, which represent a precious resource to reduce the risk of human failure due to cognitive overload, free up human resources for tasks demanding higher cognitive functions, and remove military personnel from dangerous environments. Nonetheless, the emerging core issue concerns how human and machines can team up in the armed forces, as the number of systems employed grows year by year.

The key of the debate lies in what should be a dynamic rather than static approach. When humans perform under high cognitive load, machines could take more of the burden off the soldier, while humans can then step back into the loop when machines must deal with high complex environments, instances which they have not been trained for, or physical requirements beyond their capabilities. In addition, enhanced teaming principles will require militaries to adapt operational concepts, as well as scientists will be require to develop system interfaces that are comprehensible for soldiers.

Challenges for the future

In a context where an enhanced AI adoption in the defense sector seems imminent, the NATO Defense College's paper "NATO-mation" cleary outlines a set of priorities for the Alliance to develop a coherent approach, with some of them that should be at the very heart of the issue.

First of all, the Alliance should establish ethical principles around which the development of these systems remains in-line with the founding principles of the transatlantic bond. This would be an opportunity to become a trend-setter in the international arena in an ethical approach towards R&D.

Second on the list, NATO Allies should work together to innovate their workforce, as the human side of the process becomes ever more crucial in a highly interactive work environment. A further focus should be given to Hacking for Defense-type initiatives, but also to the support of creative individuals and innovators of the sector.

Third, the Alliance needs to develop new concepts and doctrines to establish clearly which fields of AI are more promising and attracts investments from a defense perspective. To this extent, simulations, exercises, and wargames are essential, also to develop common standards, approaches, and priority areas among Allies.

The fourth point involves maintaining NATO and Allies' technological edge over the adversaries. Reinvigorating investments in R&D is the very first condition, but promoting cooperation as well as coordination on investments and reforms must not be forgotten.

Finally, the pressing issue of arms control. The Alliance has historically played an important role in deterrence and defence as a forum for discussion, and the field of AI must not be an exception. With the adoption of AI becoming pervasive and the rise of Lethal Autonomous Weapon Systems (LAWS), Allies should pay attention at identifying potential multilateral solutions which preserve international stability.

As a matter of fact, the Alliance needs more than ever cohesion and collaboration to face the multiple challenges deriving from technological revolutions. But as Ambassador d'Aboville precisely pointed out in the NDCF Game Changers 2020 Dossier:

"NATO offers proven consultative mechanisms and a unique network for collaboration on defence and security questions, being a natural platform for collaboration. […] But for such a debate to be productive, one has first to convince the decision makers and the public in the Alliance that these technologies applied to defence have an increasing momentum on their own, and, if we want to redirect it towards our own security interests (or convince others that there is a potential shared interest through arms control), we cannot be complacent or ignore facts. Denying ourselves these capabilities will not stop potential adversaries in pursuing them for their own interests."

3. The NATO 2030 process

The clouds looming over the horizon suggested by Ambassador d'Aboville can be find also in the NATO 2030 Final Report written by the Reflection Group appointed by the Secretary General. The recent assertiveness of China occurs also in the technological realm, as Beijing plans to become a world leader in Artificial Intelligence by 2030 as well as the world's leading technological power by 2049.

Nowadays, maintaining the aforementioned technological edge is crucial for the Alliance to ensure its ability to deter and defend against potential threats and to remain the world's most effective security provider. To do so, NATO has to increase the pace and scale of its political focus on the area of Emerging and Disruptive Technologies (EDTs), since the launch of the Emerging and Disruptive Technologies Roadmap in 2019 had a limited impact.

Also NATO Secretary General Jens Stoltenberg called for support for Transatlantic defense innovation and interoperability in his Food for Thought paper, in an effort to identify and work with Allied start-ups addressing cutting-edge dual-use emerging and disruptive technologies.

Besides reforming internal practices and establishing tools for consultation and dialogue on EDTs – positioning the Alliance at a leader of the debate, a relevant point of the Report is devoted to collaboration with the private sector, a need stressed also by the NATO 2030 Young Leaders. In this sense, consistent synergy could be achieved through:

- A NATO-hosted digital summit of governments and private sector, to identify gaps in collective defence cooperation in security-related AI strategies, norms, and R&D, and safeguard against the malign use of these technologies;
- Mentoring and training partnership with selected tech firms, as well as building new ones with industries, academia, and NGOs.

Moreover, the Reflection Group suggests the creation of a North Atlantic equivalent of the U.S. DARPA or European Defence Fund (EDF) to encourage and sustain innovation in strategic areas among Allies. Such an initiative should be linked to the industry and the private sector, thanks to a dedicated Advisory Group for Small and Medium Enterprises (SME) of the NATO Industrial Advisory Group (NIAG) to keep up with technological advancements.

Finally, as expressed by both the research groups of the NATO 2030 initiative, the Alliance should elaborate an ethical framework for technologies that are likely to overcome the experimental threshold such as biotechnologies and AI. How to develop, test, and implement emerging and disruptive technologies for military and security use should be at the centre of the debate.

4. The 2021 NATO Summit

SG Stoltenberg's call for cooperation on dual-use technologies can be retraced in the Brussels Summit Communiqué issued by the Head of State and Government of the 30 Allies. As agreed, foster technological cooperation, improve interoperability and encourage the development and adoption of new technologies (including AI) is a concrete goal for the Alliance. In order to achieve this objectives, the Allliance decided to:

- Launch a civil-military Defence Innovation Accelerator for the North Atlantic;
- Establish a NATO Innovation Fund, where Allies can support start-ups working on dual-use emerging and disruptive technologies in security-related fields.

A further substantive point lies on the adoption of a NATO strategy to foster and protect EDTs. Leveraging on the aforementioned 2019 EDTs Roadmap, the strategy outlines a clear approach for identifying, developing, and adopting EDTs at the speed of relevance, based on the principles of responsible use and in accordance with international law.

Allied Leaders also agreed on the extension of partnerships, deepening the relations with the private sector and academia. Once again, collaboration between the private and the public sector seems to be the cornerstone for the adoption of EDTs in the defense sector.

5. Conclusions

Artificial Intelligence promises to bring several benefits to the defense and security sector for the years to come, but for an effective adoption NATO has to take concrete choices and clear several doubts.

First, what are the applications NATO and Allies needs in the military domain? Since machines are not actually able to understand the context, the concept of Artificial General Intelligence seems to be a *chimera*, but it still meets several supporters in the academia and research. The Alliance needs to work effectively with all its members to establish what technologies better fit with the operational needs in order to avoid a waste of investments.

Second, how to promote technological innovation R&D and innovation among all 30 Allies? As argued, Artificial Intelligence needs powerful software capabilities, the *crème de la crème* of scientists to build the best algorithms, and a huge availability of data. The Alliance should analyse the state-of-the-art in all Allied countries, coming out with a deep understanding of what is the competitive advantage of the single nation and then coordinating the development of capabilities through cooperation within the NATO umbrella.

Third, how to avoid duplication and make investments pay off? As history teaches, the development of AI technologies was often ignited by massive investments from the public sector. NATO should take into account the existence of dedicated national agencies in some of its countries, in order to avoid the duplication of structures and resources and sustain less-developed realities.

Fourth, what ethical approach to AI? Serving as a unique forum for consultation and cooperation, the Alliance should retain its privileged position among Allies, helping with the creation of common R&D and use standards and procedures through open international dialogue. Only shared agreements, involving the private sector, the NGOs, the academia, and tech firms, guarantee a balanced and proportionate handling of EDTs.

Federico Berger

Social Media Intelligence (SOCMINT) Analyst for the Italian cyber security firm TS-WAY Srl since 2021. He previously served as Communication Officer and Disinformation Analyst at the NATO Defense College Foundation. Since 2020, he is enrolled in the 360/Digital Sherlocks Training Program of the DFRLab of the Atlantic Council.

NATO Foundation
Defense College