Artificial Intelligence in the European Union: Choosing the Right Path

By Nicolas Mazzucchi

Dr. Nicolas Mazzucchi, Research Fellow at the Fondation pour la Recherche Stratégique (FRS) in charge of cyber, energy, and primary goods issues

Artificial intelligence (AI) has been defined by Marvin Minsky as, "the science of making machines do things that would require intelligence if done by men." AI could be considered a game-changer in most activities as it would address most human activities when mature. In the military, the use of AI could be considered not only an enhancer but a strategic leap, as these technologies would complement the work of soldiers and experts. AI-based technologies could be present from the HQ to the forefront of the battlefield. As a consequence, the race for AI is open between major powers. Considering this framework, the European Union (EU) must enter the competition for AI with its specific areas of interests, according to its own goals.

AI: From Buzzword to Strategic Issue

At present time, AI remains mostly an in-development family of technologies. Very few genuine AI applications are available, especially in the military, and those are mostly based on connectionist technologies making an extensive use of data to achieve a proper result. Moreover, on-the-market AI solutions mostly use structured data making them of little use for the military. Having an autonomous vehicle that can only follow routes with road signs is a problem for vehicles intended to be used off-road in the desert.

Nevertheless, the most promising AI-based technologies, which provide support to the decision-maker, would revolve around symbolic AI, which is currently under-developed. Because developers, from GAFAM (Google, Apple, Facebook, Amazon, and Microsoft) and other major companies remain focused on technologies that can be quickly released to the market, amount of funding on symbolic AI appears limited. Here is a clear opportunity for public and private spending to complement one another, allowing research and development to achieve the convergence of symbolic-connectionist AI.

The position of EU countries regarding the development of AI-based technologies appears to be far behind the two superpowers: China and the United States. As demonstrated by the number of patents and the figures on public and private investment on AI, there is a gap that seems impossible to fill, unless EU policymakers can clearly decide on supporting specific technologies. Alongside this issue, the EU has to choose how it seeks to regulate AI-based technologies in the military at a global level, including technological and industrial forums.

A Follow-Up of EU Global Orientation on Cyber Issues

AI is a cyber-based family of technologies and relies mostly on two elements: computer processing capabilities and availability of data. As the technology gap between European industries and U.S. or Chinese industries is widening, the risk of a technical lag of Europe in AI is high. As Europe did not encourage the rise of major data processing companies, following a competitive path on pure computation power or data management seems to be unrealistic. Nevertheless, the EU has not been inactive on cyber issues and technologies, adopting regulations on the use and security of cyberspace and data for years.

Regarding the three pillars of information management – availability, integrity, and confidentiality – the European Union made the choice to focus on confidentiality. The recent European regulations on data and cybersecurity emphasize this choice, as both the Network and Information Security (NIS) directive and the General Data Protection Regulation (GDPR) are focused on protecting the privacy of European citizens. The extension from a cybersecurity policy dependent on critical infrastructure operators to one based on data and information providers is a major evolution of Europe toward the protection of Europe and its citizens.

GDPR especially is considered a first attempt for the EU to implement a regulation with extra-territorial consequences. Having the upper hand on the confidentiality of data helps the administrations to control the use of European data by private companies.

Which Technologies to Focus On?

As a consequence of EU strategic orientations on both cyber issues – especially regarding data and the development of military technologies under European Defense Agency or Permanent Structured Cooperation (PESCO) – EU policymakers are taking a deep look at AI solutions. Armed forces all over Europe, especially France and Germany, are considering the use of AI-based technologies to enhance their operations and limit the gap with major non-EU military powers. According to national strategic documents, these technologies may be used in nearly all military functions, from intelligence to cybersecurity or predictive maintenance. Nevertheless, with this wide area of application, there is the need to focus on specific technology issues to avoid the inefficient "spreading" of investments, especially with national priority divergences.

To be coherent with prior policy positions, it seems that the EU should focus on AI explicability, as this is a major issue. Explicability is an important feature for the training of AI with a wide variety of data to achieve a certain agility of the system. These AI technologies could provide both agility and sturdiness for the systems they would equip, especially considering the possibility of deceiving or jamming the recognition patterns. As the US DARPA is doing with several research programs, the EU – through the European Defense Fund – should have a clear focus on this strategic issue.

Second, the EU should also focus on the certification of AI results. As some military AI would be used on the battlefield, the need to ensure that the results of AI processing are not corrupted is a major concern. In terms of cybersecurity products, the EU and most of the member states have been able to ban non-compliant products from Europe. This policy could be extended to AI-based technologies, requiring a European body of AI scientists to evaluate the compliance of various technologies. This ex-post strategy appears to be the most adequate balancing of past EU cyber policy and the limits of European military industries. This specific orientation would also manifest a specific European position at the global level regarding AI technologies in the military, charting a third way between the interdiction of autonomous systems and their unrestricted use.