Wilfried Martens Centre for European Studies

January 2021

IN BRIEF

Thinking Europe, our Common House

#StaySafeStayInformed

Artificial Intelligence and Western Defence Policy: A Conceptual Note

Edward Hunter Christie

Artificial Intelligence (AI) has emerged as the main engine of growth of the Fourth Industrial Revolution, owing to its naturally cross-cutting, general-purpose nature. From a military perspective, the range of potential applications is at least as vast as the current range of tasks that require human cognition, e.g., analysing and classifying visual data, organising logistics, operating vehicles, or tracking and engaging hostile targets. How can Western nations – by which I mean those nations that are members of either NATO or the European Union (or both) – make the most out of the rise of AI, bearing in mind its potential defence applications?

The re-emergence of great power rivalries – in particular, the challenges posed by China and Russia – should clearly encourage us to pursue close transatlantic cooperation. But to ensure that such cooperation can meet its full potential, it will be necessary for policymakers to identify the right baskets of issues to bring to the table. Because AI is so cross-cutting, affecting every industry and area of activity, designing adequate policies requires an ability to integrate and connect policy discussions from an unusually broad range of different national ministries and of international institutions, including both the EU institutions and NATO. The goal of this note is to lay out some conceptual markers that will hopefully support this re-flection process. To that end, I propose an analysis according to five pillars: Facilitation, Investment, Adoption, Regulation, and Protection.

The five proposed pillars defined

Facilitation is about lifting barriers, being reform-oriented, and embracing change, in the government sector, the market, and society at large. **Investment** is about financial resources, including both increased public funding and measures to further mobilise and incentivise private investment. **Adoption**, from a government perspective, is about the deployment and use of technology within government institutions. In the case of AI, this is closely related to the broader challenge of digital transformation and implies investments in information and communications technology (ICT), infrastructure and skills, relevant process innovation and structural reforms, and policy adaptation. **Regulation**, including standardisation, governance arrangements, and legislation where relevant, is a necessary ingredient for successful technological change, but it requires careful calibration and timing. Regulate too much or too quickly, and promising innovations will be stymied. Regulate too little or too slowly, and returns on investments fall, due to frag-mentation of standards and practices, lack of quality control, and inappropriate risk management. **Protection**, last but not least, concerns measures that ad-dress the contested nature of the global technology market, notably related to intellectual property, in-vestment security, and the national and collective security interests of states.

The two main pillars for defence institutions: adoption and regulation

From the perspective of defence institutions (national institutions, as well as NATO bodies and the Euro-pean Defence Agency), the two dominant pillars are Adoption and Regulation. Adoption focuses on the resources, investments, programmatic activities, and internal processes and reforms to ensure well-developed and well-designed AI-enhanced capabilities. Many practical questions arise in the context of adoption. For example, should defence institutions create new internal structures devoted specifically to AI, or should newly hired or re-trained staff members grow the ranks of existing structures? In terms of internal processes, as AI development is naturally a software-intensive and data-intensive activity, practitioners will typically opt for Agile development models. Does this require further internal adjustments regarding traditional capability development, defence planning, or defence budgeting practices? In parallel, defence institutions naturally learn from pilot projects, from experimentation, and when capabilities are more mature, from exercises. What specific projects and programmes would be most useful at this time? Which ones should best be pursued collaboratively, with several allied or partner nations? And under what conditions should such collaborative work be pursued with NATO support, or EDA support? These questions are left deliberately open for further reflection on the part of relevant practitioners and experts.

Regulation, again in the defence context, refers to a set of policies and frameworks that would specify how AI is to be developed and used. This includes military concepts and doctrines, standards to ensure interoperability, and principles of responsible use. The notion of responsible use refers to commitments that sovereign states may choose to make, bearing in mind the commitments of other states. This includes, but is not necessarily limited to, compliance with existing international law and international humanitarian law. The most notable international effort in this area to date has been the consultations held under United Nations auspices by the Group of Governmental Experts on Lethal Autonomous Weapon Systems. From a technical perspective, AI capabilities are adaptable and versatile. This is what makes them so attractive in the first place, but it also leads to new challenges. How should technical validation and verification processes be adapted to cope with AI? What new testing facilities, procedures, and standards do nations need to move forward in this area? Relatedly, the pursuit of principles of responsible use naturally spills over into questions of engineering principles. Therefore, states will also wish to consider the feedback loop between commitments made in international fora, and the technical characteristics of the systems in question.

Towards a whole-of-government[1] approach

Additionally, one needs to understand both the differences and the potential synergies between civilian and military-oriented activities. While state funding, and notably defence funding, played a key role in the early development of computing and of the Internet during the Cold War, the current wave of AI, which is mainly centred on Machine Learning and Deep Learning, is overwhelmingly unfolding in civilian-oriented institutions and for civilian-oriented uses. Pursuing AI is a twin-track process, focused on achieving both economic competitiveness and military capabilities, and it is unfolding in an international environment that is largely liberalised and globalised, but also increasingly competitive and contested. A whole-of-government approach is therefore needed in order to appropriately design public policy efforts.

A best-practice example, in my view, is the US National Security Commission on Artificial Intelligence (NSCAI). Leveraging both former government officials and industry leaders, this expert body was man-dated by the US Congress to "*consider the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States*". The mandate of the NSCAI has allowed it to study a broad range of potential policy initiatives and to generate recommendations addressed to whichever government bodies or agencies were best suited,

[1] An approach that mobilises collaborative, rather than competitive or disjointed, contributions from multiple departments and agencies of government in the pursuit of a common goal.

including but not limited to the Defense, State, Homeland Security, and Commerce Departments, and national agencies such as the National Science Foundation, among others.

Whole-of-government thinking, by its very nature, has to occur mainly in national capitals, but both the EU institutions and NATO can provide substantial added value to national efforts, and it will be desirable for nations to encourage this. While calls for greater NATO-EU cooperation are common and should be pursued, an additional avenue for greater cooperation among Western nations should be the OECD. The OECD's membership spans the Euro-Atlantic region, and the OECD brings to the table considerable expertise on digital economy, innovation, and science and technology policies.

Selected Policy Recommendations

In addition to the concepts and suggestions outlined above, certain more specific recommendations are offered in this final section. These recommendations fall under three of the five pillars outlined earlier, namely Facilitation, Investment, and Protection. The recommendations are aimed at generating further re-flection and support for policy coordination among Western nations on both sides of the Atlantic.

Facilitation: The development of AI for defence ap-plications in a multinational context naturally raises the question of transfers of both technologies and data among allied and partner nations. Facilitation measures may therefore be focused on reforms that would make such transfers easier. One specific area of reflection concerns obstacles to the sharing of relevant datasets for the training of Machine Learning algorithms. For the European Union, while existing legislation such as the GDPR provides clear limitations for civilian-oriented activities, it is less clear how EU Member States and their allies and partners out-side the Union, including the United States, should organise and regulate the sharing of relevant datasets for defence purposes. Targeted analytical and policy design efforts would be particularly useful in this area, possibly leading to a bespoke agreement to facilitate multinational efforts among EU Member States as well as among NATO allies, including the United States.

Investment: Western governments have an interest in mobilising financial resources, both public and private, for the development of AI. Increases in relevant public budgets for both basic and applied scientific and technological research would be desirable. Potential synergies and complementarities between civilian-oriented and defence-oriented research efforts should be explored. Concerning multinational cooperation, it would be interesting to give further, more detailed consideration to the NATO Reflection Group proposal (see page 31 of the Group's final report) to develop a transatlantic defence research fund, modelled on the US Defense Advanced Research Pro-jects Agency (DARPA) and on the European Defence Fund (EDF), which could support innovation efforts in strategic areas among allied nations. In addition to traditional state funding, a major strand of current pol-icy thinking recognises the large potential of both market mechanisms and private sector capital in enabling technological innovation. The United States has been particularly successful in developing a large and vibrant private venture capital ecosystem. Drawing on this experience, state venture capital instruments have also been developed, a well-established example being In-Q-Tel in the United States, where public funds are used to make mid- to long-term equity investments in promising technology companies. Most recently, France has announced the creation of the Fonds innovation défense, a state venture capital instrument aimed at investments in promising small and medium enterprises in dual-use technologies which will also allow for private sector add-on investments. Nations on both sides of the Atlantic may wish to further consider such instruments from a multinational perspective as well. A transatlantic defence in-novation venture fund, which would be open to private sector investors from both Europe and North America, and perhaps other like-minded nations, would be worth exploring.

Protection: The strategic objective of Western nations should be to remain collectively ahead of any potential rival powers. In practice, this means that European nations have an interest in closely collaborating with the United States, while adopting a healthy scepticism with respect to major non-

Western powers which do not share our common values. It is public knowledge that those powers conduct activities against Western targets, notably aimed at the acquisition of cutting-edge technologies, as was recently illustrated by the expulsion of two Russian nationals from the Netherlands for science and technology espionage. Several policy counter-measures are relevant in this context. Increasingly, Western nations are prepared to tighten regulations and screening mechanisms relating to foreign investment. Efforts should be undertaken to identify and learn from national best practices, regarding both policy design and enforcement. In that context, counter-intelligence efforts are naturally becoming more relevant and must be well-resourced. In addition, an interesting development is the US Department of Defense's Trusted Capital Marketplace initiative. The goal of the initiative is to generate a boundary between trusted and non-trusted prospective private investors with an interest in sensitive technology companies. In effect, gaining recognition as a 'trusted investor' would operate like a certification attesting to the correct implementation of a standard of good practice in terms of financial and national security propriety. Extending this notion to a multinational context, one may consider how such a good practice standard could be developed and recognised among like-minded nations, on both sides of the Atlantic, thus facilitating mutual investments in innovation ecosystems that involve potentially sensitive technologies.

Concluding remarks

The common thrust of the recommendations above is the pursuit of whole-of-government action and whole-of-government thinking in the service of the twin goals of Western security and Western prosperity. The nature of the AI challenge – the fact that we are experiencing the rise of a major cross-cutting technology in a context of renewed global competition – requires the ability to combine and align policies, ranging from internal and external economic instruments to military capability development choices. Potential adversaries already pursue, each in their own way, an authoritarian civil-military collab-oration model. It is up to the West to come up with a democratic one.

Edward Hunter Christie *is a researcher at the Vrije Universiteit Brussel (VUB) and a Research Associate of the Wilfried Martens Centre for European Studies. After working in research and in EU affairs, he served as a NATO official from 2014 to 2020, ending his tenure with the role of Deputy Head of Innovation. In that capacity, he was the author of NATO's White Paper on Artificial Intelligence.*

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party (EPP), dedicated to the promotion of Christian Democrat, conservative and likeminded political values.

This publication receives funding from the European Parliament.

Editor: Vít Novotný, Ph.D.

Wilfried Martens Centre for European Studies
Rue du Commerce 20
Brussels, BE – 1000
http://www.martenscentre.eu