Article

Wilfried
Martens Centre
for European Studies

European View
2022, Vol. 21(1) 13–21
© The Author(s) 2022
DOI: 10.1177/17816858221089372
journals.sagepub.com/home/euv
SAGE

Defence cooperation in artificial intelligence: Bridging the transatlantic gap for a stronger Europe

Edward Hunter Christie

Abstract

This article provides a brief overview of European and transatlantic defence cooperation in the area of artificial intelligence. As states race forward to achieve superiority in artificial intelligence, including its military applications, NATO allies and partner nations on both sides of the Atlantic have a strong incentive to cooperate closely and ensure the collective West can maintain its technological edge. However, large gaps remain between the US and the EU on certain key indicators. To ensure greater European performance and relevance, it is desirable to focus on two strategic priorities: investment volumes, both public and private, which need to be significantly increased; and the full use of collaborative mechanisms involving the US.

Keywords

Transatlantic relationship, Defence cooperation, Artificial intelligence, NATO, EU

Introduction

Artificial intelligence (AI) is the ability of machines to perform tasks that typically require human intelligence—for example, recognising patterns, learning from experience, drawing conclusions, making predictions or taking action—whether digitally or as the smart software behind autonomous physical systems (Reding and Eaton 2020, 14).

The range of potential military applications is at least as vast as the range of tasks that require human cognition, for example analysing and classifying visual data, organising logistics, operating support vehicles, or tracking and engaging hostile targets (Christie

Corresponding author:
E. H. Christie, Finnish Institute of International Affairs, Arkadiankatu 23 B, Helsinki 00100, Finland.
Emails: edward.hunter.christie@fiiafellow.fi; edward.hunter.christie@gmail.com

2021b, 84). States are racing to achieve superiority in the AI domain (Lin-Greenberg 2020). Furthermore, like other digital technologies, AI diffuses rapidly and cheaply across areas of human activity and across borders. Nevertheless, as with other technological transformations, states with greater resources and levels of effort, and better policies, will reap the benefits of technology adoption more rapidly than others.

In an alliance context, matters pertaining to cooperation and interoperability take centre stage. The good news is that Europeans are not starting from scratch. European states that are members of NATO can rely on decades of experience with the Alliance's mechanisms of consultation and collaboration. In addition, European states that are members of the EU can pursue collaborative activities through the European Defence Agency (EDA). Furthermore, EU funding is available through the European Defence Fund for defence research and capability-development activities.

At NATO the key processes address, most notably, the areas of defence research, military transformation, capability development, military–technical standardisation, and defence planning and capability targets. For these areas of work, formal consultative mechanisms—committees in which each Ally has a voice—include the Science and Technology Board, the Military Committee, the Conference of National Armaments Directors, the NATO Standardisation Board, and the Defence Policy and Planning Committee. Each of these committees relies on support staffs and structures. Of particular interest when considering AI are the Science and Technology Organisation, which has several facilities and is led by the Office of the Chief Scientist at NATO Headquarters; and, Allied Command Transformation. The latter, including its Innovation Hub, plays a particularly central role in driving innovation and force transformation for the Alliance. In addition, two staff units created in 2019 are of particular importance, namely the Innovation Unit and the Data Policy Unit, both of which are within the Emerging Security Challenges Division of the NATO International Staff. The Innovation Unit provides thought leadership and initiatives to accelerate technology adoption, while the Data Policy Unit provides policy thought leadership on how to treat data as a strategic resource. The Innovation Unit designs new initiatives for the promotion and financing of defence-related innovation. A notable achievement in this area was the creation of the NATO Innovation Fund (*NATO* 2021).

In the EU context, the EDA plays a central role in several areas of work. Among other activities, the EDA supports defence research cooperation, defence standardisation and pooled procurement programmes, while also contributing to the EU's Capability Development Plan and Coordinated Annual Review on Defence (Fiott 2018, 287). Most of the EDA's functions are broadly analogous to ones that exist at NATO. Of particular interest is the intention to create a new Defence Innovation Hub within the EDA, as announced in the EU's November 2021 draft Strategic Compass (European External Action Service 2021, 23).

Before proceeding, it is worth spelling out the extent to which European security is dependent on NATO and in particular on the US. Of the EU's 27 member states, 21 are members of NATO. These countries account for about 93% of the population[1] of the EU.

Within NATO, those Allies that are also EU members only account for about 20% of total defence expenditure across the Alliance, while the US alone accounts for about 70% of the same total.[2] Beyond these aggregate indicators, it is furthermore the case that the US is considerably ahead of the EU in terms of practical adoption of AI. For illustration, in 2020 US private-sector investment in AI was around $23.6 billion, but was only $2 billion in the EU, implying a ratio of 12 to 1 in favour of the US (Zhang et al. 2021, 96). Scientific output indicators offer a more nuanced picture. In 2019, the EU accounted for 16.4% of the world's peer-reviewed AI publications, ahead of the US with 14.6%, while China occupied the top spot with 22.4% (Zhang et al. 2021, 20). On the other hand, if one measures research output in terms of publications on the Arxiv database, the US is ahead of the EU (Zhang et al. 2021, 33) by a ratio of almost two to one, which is nonetheless much less than the large gap in private investment mentioned above. That the EU performs similarly to the US in terms of scientific research, but far less well in terms of investment and commercialisation of new digital technologies, is an old problem which has proven very difficult to address, whether at national or EU level (Baroudy et al. 2020).

In the following sections, I offer reflections on three challenge areas for European and Allied defence institutions: interoperability challenges, international security challenges and investment challenges. These three challenges are effectively interdependent. While interoperability is a permanent goal in an alliance context, be it NATO or the EU, it is particularly salient in cases of rapid technological change, such as with AI, as there is a need for a higher tempo across areas of activity. Heightened international security challenges likewise increase the need for urgency to ensure that Western nations do not fall behind potential adversaries. Investment, in turn, is the engine for rapid change, enabling the dynamic adoption of new technologies, relevant capability-development activities and other adaptations along the value chain of military activities. Overall, my central argument is that the confluence of rapid technological change and heightened international security challenges requires a higher pace of change and adaptation that can only succeed if serious investments are made on both sides of the Atlantic.

Interoperability challenges

Interoperability can be defined as 'the ability of systems, units or forces to provide services to, and accept services from other systems, units or forces and the use the services so exchanged to enable them to operate effectively together' (Dufour 2018, 1).

The first general challenge to interoperability is the overall gap between the US and Europe in terms of total defence investment, as well as in terms of civilian technological attainment with respect to AI and related technologies. There is no single solution to this problem, which is much broader in scope than traditional military–technical standards, such as those pursued in the NATO context through existing mechanisms. For this broad challenge, overall policy decisions relating to national investment choices and technology policy coordination between the two sides of the Atlantic are of particular importance. Further discussion of this follows in the sections on investment challenges and international security challenges.

A second challenge to interoperability is that, as far as digital technologies are concerned, the civilian sector of the economy, on both sides of the Atlantic, is more advanced, more dynamic and also not especially oriented towards meeting military needs. For decades, the military sector has represented only a very small share of the total sales volume of the computing and semiconductor industries. The same pattern is repeating itself currently with AI. This stands in great contrast to narrower dual-use technologies, for example aerospace, where the military sector remains inherently important. With digital technologies, defence institutions are under much more pressure to either adapt to civilian industry products and standards or to pay a significant premium to suppliers to secure military-grade equipment and software.

A third challenge to interoperability lies in how AI is implemented in practice. To set up a bespoke machine-learning algorithm in a given data environment, best practice in the software industry is to pursue some variant of 'agile' development. This involves a very different product-development cycle, essentially proceeding with multiple rapid iterations of an imperfect product that is released in preliminary versions and later revised—like software products released in various 'beta versions'—with upgrades developed over time. This contrasts greatly with the traditional production of major military platforms, which puts a premium on strict quality control and compliance with requirements at every development step—an approach referred to in the software industry as 'waterfall' development (Christie 2021b, 87). Agile product development may pose challenges to interoperability. Unless very tight standards are applied, there is a considerable risk of divergences in how different national institutions go about solving a particular AI or data analytics problem.

With large traditional military platforms there are long time frames during which states can take coordination steps, either by purchasing the same platforms, or by building consensus in terms of requirements and standards. However, when a comparatively small team works dynamically to generate an algorithmic solution to a particular problem in a matter of weeks or months, traditional coordination through existing consultation mechanisms may pose risks to the speed advantage inherent to agile development. Conversely, once a solution has been developed, its adoption in somewhat different environments may be challenging for a range of technical reasons. None of these issues is insurmountable, but they do pose, in a new light, classical trade-offs between the benefits of inventiveness and dynamism, on the one hand, and those of imposing constraints through standards and other harmonising measures to ensure that new products can be broadly used and shared on the other. In the case of AI, a typical observation is that there are many excellent prototypes and pilot projects in numerous defence institutions, but there are also serious outstanding challenges in terms of scaling up to enterprise-wide solutions, let alone Alliance-wide solutions.

Finally, the question of ethical AI—or responsible AI—generates considerable attention on the part of governments and civil society. In response, NATO sought to establish a consensus on certain essential principles, referred to as Principles of Responsible Use, which build on emerging national commitments. These principles were endorsed by Allied governments in October 2021 (Stanley-Lockman and Christie 2021).

International security challenges

Both EU nations and the US are exposed to the same global environment and to similar strategic concerns, at the confluence of rapid technological change and global power shifts. Starting from around 2018, policy discourse in the US became particularly focused on fears of being overtaken by China technologically and militarily. A good illustration of these fears is a 2020 statement by the Director of the Federal Bureau of Investigation, who accused the Chinese government of 'fighting a generational fight to surpass our country in economic and technological leadership' and of 'taking an all-tools and all-sectors approach . . . that demands our own all-tools and all-sectors approach in response' (Wray 2020).

For military AI, China poses the greatest challenge to Western nations (Kania 2019). However, Russia is also actively pursuing such capabilities (Zysk 2021; Engvall 2021), including through espionage, for example against the Netherlands (AIVD 2020) and France (Follorou 2021).

Nations on both sides of the Atlantic have recognised the rising challenge of Chinese and Russian government-sponsored industrial espionage aimed at the illegitimate acquisition of cutting-edge Western technologies. And both the US and the EU have adopted strengthened legislation in several key areas, including on the protection of trade secrets, on export controls for dual-use items and on the screening of foreign direct investment (Christie 2021a). Another relevant area of work is measures to better protect the university and research sector from espionage. A new toolkit of recommendations now exists at EU level (European Commission 2022).

Investment challenges

As noted in the introduction, there is a significant gap between overall US and European defence spending levels. This general pattern also holds for defence research and development spending. In 2020, EU spending in this area amounted to €8 billion (EDA 2021). For the US, with caveats as to comparability, expenditure for 'research, development, test and evaluation' totalled approximately €90 billion[3] in the 2021 fiscal year (from October 2020 to September 2021), or about 10 times more.

Investment challenges go beyond issues of scale. The US also has greater experience in the setting up and operation of structures to promote both military and dual-use innovation. While the best-known institution is the Defense Advanced Research Projects Agency, other US government structures are also relevant in discussions on fostering innovation in AI for military applications. A much-discussed example is In-Q-Tel, which was originally set up as the state venture-capital arm of the Central Intelligence Agency. To illustrate the influence of the In-Q-Tel example, one may note that both its current Chief Executive Officer, Chris Darby, and one of its former Chief Executive Officers, Gilman Louie, served among the 15 commissioners of the National Security Commission on Artificial Intelligence.[4] This was a temporarily created expert commission mandated by the US Congress to provide policy recommendations for a whole-of-government and whole-of-society approach for US AI policy.[5]

With In-Q-Tel, the idea is to learn from private-sector practices in the area of venture-capital investment and repurpose them for state needs and more patient time horizons. A supported company should pursue product development strategies aimed at serving both civilian markets and government needs. In this way, rather than effectively taking over a commercial company and limiting its growth potential to future government contracts alone, the government body encourages an intermediate trajectory made up of mixed revenue streams, in the hope that this will generate greater returns to scale and higher efficiency thanks to the disciplining effect of private-sector competition. Conversely, the advantage of this approach as compared to not intervening at all is that the commercial company will integrate current and likely future government needs into its product and business-development strategy, rather than ignoring them and finding itself, at a later date, unable to supply the government sector according to the latter's requirements.

A related issue which falls between what can be achieved with new investment instruments and new protections that can be assured through the screening of foreign direct investment is the provision of investment from trusted private investors to the technology sector. Certain technology companies that are not part of the traditional defence industry may be developing dual-use products that are of potential interest to the defence sector while having limited awareness of national security concerns. This may make them vulnerable targets for both licit and illicit attempts to acquire their technologies on the part of foreign state actors. At the same time, their business development needs may lead them to seek investment from any potential source, thus exposing them to potential risks. To respond to this challenge, the US Department of Defense has launched a scheme called the Trusted Capital Marketplace (US Department of Defense 2021a).

Building on these considerations, the NATO Innovation Unit has developed two new instruments for Allied use which were announced to the public in October 2021 (NATO 2021a; 2021b). Both instruments aim to foster technological innovation with a deliberate focus on dual-use applications and on enterprises with mixed (potential) revenue streams. The first instrument is the Defence Innovation Accelerator for the North Atlantic (DIANA), which is a NATO instrument, that is, it involves the participation of all 30 NATO Allies. The second instrument is the NATO Innovation Fund, which in NATO terminology is a 'multinational' instrument, namely one that Allies freely opt into.

DIANA will aim to accelerate the adoption of dual-use technological solutions through several interlocking components.[6] First, it will develop a network of national organisations, in particular test centres and innovation accelerators. Second, it will competitively select private-sector innovators and allow them to use national organisations in the network to interface with military end users and military capability-development specialists. Third, it is envisaged that DIANA will provide mentorship and education services for private innovators to familiarise them with the opportunities and responsibilities inherent to the defence and security sector. Fourth, DIANA will develop a database of trusted financial investors from Allied nations and support matchmaking between investors and innovators. Fifth and finally, DIANA will also provide expert advice on defence and security innovation to all relevant stakeholders, including private-sector and academic entities.

Regarding the NATO Innovation Fund, 17 Allies had opted into the Fund as of the date of its announcement in October 2021. The participating Allies will inject up to €1 billion into Allied innovation ecosystems over the next 15 years. The Fund aims to attract additional private investments due to the de-risking effect, both financial and technological, thanks to state co-funding and diligence and screening efforts. The funds are intended to be used for long-term support of 'deep tech' innovative companies, that is, for advanced research into AI, quantum and related technologies that may have both military and civilian applications. Due diligence and security screening practices will aim to ensure that both private investors and fund recipients are trusted entities.

Conclusions

Much has already been achieved in terms of new structures, new initiatives and new policy developments to support the collaborative adoption of AI among NATO Allies and EU member states. In addition to pre-existing structures and mechanisms at both the NATO and EU levels, which have ensured that nations are not starting from scratch, national defence institutions are already able to refer to common policy commitments and to options, whether through NATO or the EDA, for research or capability-development activities. At the same time, ensuring a competitive edge in AI is a truly whole-of-government effort which requires considerable cross-over between the military and civilian realms.

Large gaps remain between the US and the EU on certain key indicators. At the same time, the gaps pertaining to research are far smaller. To ensure greater European performance and relevance in AI in general, and its defence applications in particular, it seems desirable to focus on two strategic priorities: investment volumes, both public and private, which need to be significantly increased; and the full use of collaborative mechanisms involving the US.

To that end, it would be beneficial for nations on both sides of the Atlantic to ensure that a clear and common vision is set out in forthcoming strategic documents, most notably the EU's Strategic Compass and NATO's new Strategic Concept. This should include clear political commitments to increasing investment, both in general and in instruments for promoting collaborative innovation. There are opportunities for 'more Europe' through the EDA and the European Defence Fund. But while pursuing those avenues, European capitals should prioritise efforts that complement and enhance transatlantic approaches, in recognition of the reality that the US remains the indispensable ally for Europe's security.

Notes

[1] Own calculations based on Eurostat population data.

[2] Own calculations based on NATO defence expenditure data.

[3] As reported in May 2021, the request for the 2022 US fiscal year was '$112 billion, which is a 5.1% increase over fiscal 2021' (US Department of Defense 2021b). This implies a level of

$106.5 billion for the 2021 fiscal year. Applying the average exchange rate for 2021, which was 1.1827, yields €90.1 billion.

4. See National Security Commission on Artificial Intelligence (n. d.).
5. The author of the present article served as the liaison between the NATO Innovation Unit and the Commission's staff in 2020.
6. The description of the intended characteristics of DIANA is based on interviews with serving NATO Innovation Unit staff.

References

AIVD. (2020). AIVD rolt spionagenetwerk op in Nederland; twee Russische inlichtingenofficieren moeten het land verlaten [AIVD rolls up spy network in the Netherlands General Intelligence and Security Service (AIVD)]. 10 December. https://www.aivd.Nl/actueel/nieuws/2020/12/10/aivd-rolt-spionagenetwerk-op-in-nederland-twee-russische-inlichtingenofficieren-moeten-het-land-verlaten. Accessed 17 February 2022.

Baroudy, K., Janmark, J., Satyavarapu, A., Strålin, T., & Ziemke, Z. (2020). *Europe's start-up ecosystem: Heating up, but still facing challenges*. McKinsey & Company. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/europes-start-up-ecosystem-heating-up-but-still-facing-challenges. Accessed 5 February 2022.

Christie, E. H. (2021a). 'Economics and technology: Emerging new threats'. Remarks delivered at the Prague Security Studies Institute, Prague, 9 November. *AI Policy Blog*. https://www.aipolicyconsulting.com/economics-and-technology-new-threats. Accessed 26 January 2022.

Christie, E. H. (2021b). The NATO Alliance and the challenges of artificial intelligence adoption. In S. Lucarelli, A. Marrone & F. N. Moro (eds.), *NATO decision-making in the age of big data and artificial intelligence* (pp. 84–93). Brussels: NATO. https://www.iai.it/en/pubblicazioni/nato-decision-making-age-big-data-and-artificial-intelligence. Accessed 26 January 2022.

Dufour, M. (2018). *Will artificial intelligence challenge NATO interoperability?* NATO Defence College, Policy Brief no. 6. December. https://www.ndc.nato.int/news/news.php?icode=1239. Accessed 26 January 2022.

EDA. (2021). *Defence data 2019–2020: Key findings and analysis*. Brussels. https://eda.europa.eu/docs/default-source/brochures/eda—defence-data-report-2019-2020.pdf. Accessed 26 January 2022.

Engvall, J. (2021). *Russia's military R&D infrastructure: A primer*. Stockholm: Swedish Defence Research Agency (FOI). https://www.foi.se/report-summary?reportNo=FOI-R—5124—SE. Accessed 5 February 2022.

European Commission. (2022). *Tackling R&I foreign interference*. Staff Working Document. https://op.europa.eu/s/vR4a. Accessed 5 February 2022.

European External Action Service. (2021). *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*. Working Document, EEAS (2021) 1169, 9 November. https://s3.eu-central-1.amazonaws.com/euobs-media/326b61261ab995993ddb7581e47aa4f3.pdf. Accessed 12 February 2022.

Fiott, D. (2018). EU–NATO cooperation: The case of defense R&D. In N. Karampekios, I. Oikonomou & E. G. Carayannis (eds). *The emergence of EU defense research policy* (pp. 281–97). Cham: Springer.

Follorou, J. (2021). La France, comme l'Europe, subit les assauts de l'espionnage russe [France, like Europe, endures Russian espionage attacks]. *Le Monde*, 13 April. https://www.lemonde.fr/societe/article/2021/04/13/la-france-comme-l-europe-subit-les-assauts-de-l-espionnage-russe_6076625_3224.html. Accessed 17 February 2022.

Kania, E. B. (2019). Chinese military innovation in the AI revolution. *The RUSI Journal*, *164*(5–6), 26–34.

Lin-Greenberg, E. (2020). Allies and artificial intelligence: Obstacles to operations and decision making. *Texas National Security Review*, *3*(2), 56–76. https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/. Accessed 12 February 2022.

NATO. (2021). NATO Allies take the lead on the development of NATO's Innovation Fund. Press Release, 22 October. https://www.nato.Int/cps/en/natohq/news_187607.htm. Accessed 30 January 2022.

Reding, D. F., & Eaton, J., *Science & technology trends 2020–2040 – Exploring the S&T edge*. NATO Science & Technology Organization. Brussels. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf. Accessed 18 January 2022.

Stanley-Lockman, Z., & Christie, E. H. (2021). An artificial intelligence strategy for NATO. *NATO Review*, 25 October. https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html. Accessed 5 February 2022.

US Department of Defense. (2021a). Department of Defense announces establishment of the Trusted Capital Digital Marketplace. Press Release, 13 January. https://www.Defense.gov/News/Releases/Release/Article/2470485/department-of-defense-announces-establishment-of-the-trusted-capital-digital-ma/. Accessed 19 February 2022.

US Department of Defense. (2021b). DOD budget request boosts research, nuclear modernization and includes 2.7% pay raise. Press Release, 28 May. https://www.defense.gov/News/News-Stories/Article/Article/2639101/dod-budget-request-boosts-research-nuclear-modernization-and-includes-27-pay-ra/. Accessed 19 February 2022.

US, National Security Commission on Artificial Intelligence. (n. d.). Commissioners. https://www.nscai.gov/commissioners/. Accessed 14 February 2022.

Wray, C. (2020). 'Responding effectively to the Chinese economic espionage threat'. Remarks at the Department of Justice China Initiative Conference, Center for Strategic and International Studies, Washington, D. C., 6 February. https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat. Accessed 5 February 2022.

Zhang, D., Mishra, S., Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., Lyons, T., Manyika, J., Niebles, J. C., Sellitto, M., Shoham, Y., Clark, J., & Perrault, R. (2021). *Artificial intelligence index report 2021*. Human-Centered AI Institute, Stanford University. March. https://aiindex.stanford.edu/report/. Accessed 5 February 2022.

Zysk, K. (2021). Defence innovation and the 4th industrial revolution in Russia. *Journal of Strategic Studies*, *44*(4), 543–71. https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1856090. Accessed 10 February 2022.

Author biography

Edward Hunter Christie *is a senior research fellow at the Finnish Institute of International Affairs and the owner of AI Policy Consulting. He served as a NATO official from 2014 to 2020, ending his tenure at NATO in the role of deputy head of the Innovation Unit.*