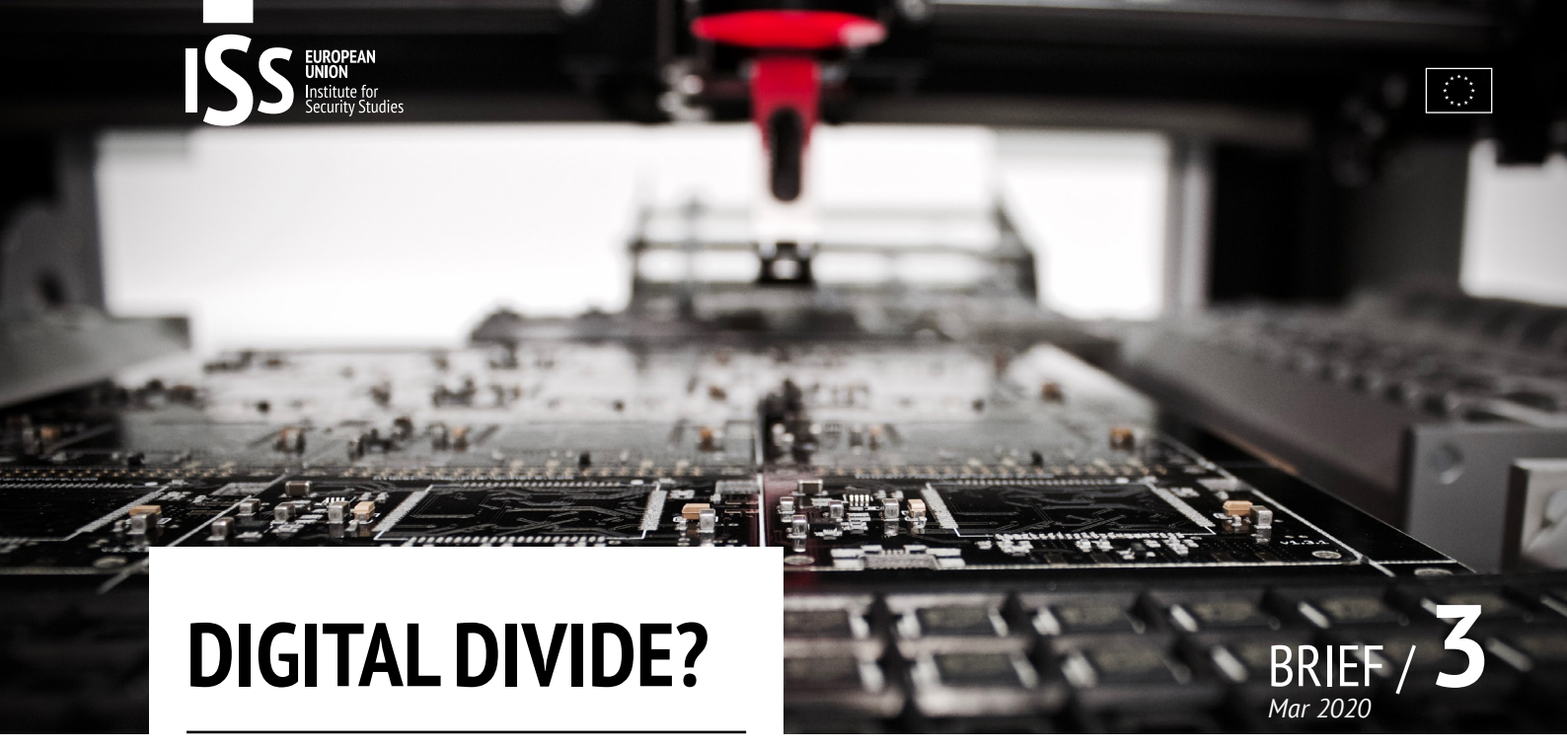


DIGITAL DIVIDE?

BRIEF / 3
Mar 2020

Transatlantic defence cooperation on Artificial Intelligence

by
Simona R. Soare
Senior Associate Analyst

INTRODUCTION

Emerging technologies, including Artificial Intelligence (AI), quantum computing, big data, 5G and biotechnology are paving the way towards defence modernisation in a growing number of states, particularly in the US, Russia and China. While AI technologies and their impact have been on the radar of European governments, there has been little scrutiny in Europe of how the evolving US approach to AI affects European defence and the broader transatlantic partnership. At the heart of the US defence modernisation programme is the *Artificial Intelligence Strategy* unveiled by the Department of Defense (DOD) in 2019. What implications does this have for Europe and for transatlantic cooperation?

In examining this question this Brief finds that cooperation with the US on the digital modernisation of defence remains a strategic necessity for Europe, but a mix of new and pre-existing dynamics in the relationship risks the emergence of a transatlantic digital divide. The Brief is structured in three parts. The first part explores the key tenets of the DOD AI

Summary

- A consensus is emerging on both sides of the Atlantic that the adoption of AI in defence is a vital security interest.
- Cooperation with the US on the digital modernisation of defence remains a strategic necessity for Europe. Nevertheless, a mix of new and pre-existing dynamics in the relationship risks the emergence of a transatlantic digital divide.
- Transatlantic AI technology and investment gaps can spill into the defence sector and erode military interoperability and deterrence.
- The EU-NATO framework may also come under pressure in the coming years to manage transatlantic differences over AI and data governance as well as diverging perceptions of the threat posed by China.

Strategy. The second part examines challenges to the adoption of AI technologies in the US, many of which are shared by European partners. The third part of the Brief explores the implications of the DOD AI Strategy for European security.

THE DOD AI STRATEGY: KEY TENETS

The 2019 DOD AI Strategy pledges an AI-enabled digital transformation of US military power in preparation for great power competition with China and Russia, both of whom are 'making significant investments in AI for military purposes' that 'threaten to erode [US] technological and operational advantages'.[1] The strategy rests on five pillars: developing AI-enabled capabilities; effective AI governance, including decentralised experimentation; creating a skilled AI workforce; leadership in military ethics and AI safety; and engagement with private partners and international allies. It is underpinned by an ethical approach and proposes a framework in which AI technologies are used to address broader security issues such as disaster management.[2]

Much like the *Third Offset Strategy* launched in 2014, the 2019 AI Strategy is driven by the strategic imperative of maintaining US military superiority and restoring escalation dominance by offsetting advanced Chinese and Russian capabilities (e.g. long-range weapons) and strategies (e.g. hybrid and anti-access/area denial – A2/AD). In this strategic environment, the US military is forced to operate along a physical, virtual and information 'competition continuum,'[3] where it engages in cooperation and competition with both its friends and its adversaries.

AI is the strategic enabler of a fully integrated digital and information military ecosystem comprising cyber, cloud and edge computing, and command, control and communications (C3)

Building on the legacy of network-centric-warfare (NCW), AI is the strategic enabler of a fully integrated digital and information military ecosystem comprising cyber, cloud and edge computing, and command, control and communications (C3). The goal is to optimise administrative and operational performance and develop a comprehensive 'networked nervous system for warfare' that uses AI to enable multi-domain operations.[4] By rapidly aggregating and concentrating power across all domains of warfare simultaneously, multi-domain operations achieve a competitive advantage over the enemy not by dominance but by presenting multiple complementary threats, each requiring a response and exposing the vulnerabilities of the adversary.[5]

The Pentagon expects AI to maximise operational impact in four main areas: information superiority, combat readiness, greater operational speed, and competitive advantage across the full spectrum of warfare, including below the threshold of armed conflict.[6] Specific AI use cases are linked to these operational needs. The DOD is experimenting with data fusion, which includes the rapid analysis of torrents of satellite imagery to produce enhanced situational awareness,[7] and the Air Force is running three programmes to develop probabilistic algorithms that model alternative scenarios to support decision-makers. The Pentagon's Preventive Maintenance (PMx NMI) project, which monitors the performance of US Special Operating Forces helicopters and conducts preventive maintenance to ensure the equipment is ready for deployment,[8] is connected to readiness requirements and pressures to reduce the ballooning maintenance costs of legacy systems.

IMPLEMENTATION CHALLENGES

The DOD wants 'as much machine-to-machine interaction as is possible to allow humans to be presented with various courses of actions for decision.'[9] However, important obstacles to successful adoption remain, including technological fragility, bias and opaqueness, limited human skills, a lack of trust in these brittle technologies,[10] and a lack of understanding about how they affect deterrence, escalation and strategic stability. Despite the Pentagon's ambitious outlook on the digital modernisation of defence, the focus of the AI strategy has been on rapidly maximising the benefits from the low-hanging AI fruit in low-consequence areas like logistics and predictive maintenance. This section focuses on three challenges the DOD is facing in implementing the AI strategy – challenges that are relevant to the European context, too.

Building reliable public-private AI partnerships

The private sector is the biggest disruptor when it comes to technological progress and outspends

governments in emerging technologies. Therefore, the DOD's ambitious digital modernisation of defence is more dependent than ever on a difficult relationship with the private sector. Numerous problems plague the relationship, including a deficit of mutual trust, different organisational cultures, poor governmental preparedness, long acquisition processes, stovepiped, missing or unreliable data, and technical and security challenges in adopting AI technologies that are optimised for commercial use.[11] In addition to International Traffic in Arms Regulations (ITAR) and export control limitations, misalignment between innovation cycles in the private and governmental sectors, suspicions among big tech companies about governmental uses of technology, and business opportunity costs are taking their toll on the relationship. The lack of governmental coordination on the building blocks for the deployment of military AI, particularly cloud and edge infrastructure and a data strategy, have further undermined the relationship with private industry. This was demonstrated recently when the DOD delayed plans to build the Joint Common Foundation (JCF), a common repository of cloud-based algorithms, models and shared data for all agencies and services. This was the result of a prolonged and contentious process[12] over the appropriation of the Joint Enterprise Defence Infrastructure (JEDI) – the DOD's $10 billion common cloud infrastructure programme that was supposed to host the common AI repository. Such examples prove that the strained relationship with civil industry is a critical limitation on DOD plans to adopt AI and shows the limits of translating economic and technological capacity into military power.

Passing the AI agility test

The Pentagon's adoption of AI is modelled on private sector experience - start small, prototype and pilot fast, scale, upgrade, and repeat. While the reform of the DOD's defence acquisition process is far from complete, the Pentagon is hard-pressed to adopt software-based solutions within three months to two years,[13] a significantly shorter timeframe than the current average of 7.5 years. The Algorithmic Warfare Cross-Functional Team, known as Project Maven – a project that used computer vision and machine learning for rapid video analysis in support of counterterrorism efforts in the Middle East – is a telling case, having moved from prototype to experimental testing, initial deployment and a first round of upgrading in under three years.

The capability development timelines for AI technologies are, nevertheless, misleading. First, they focus on prototype and experimental development that results in limited deployment, usually with the unit that piloted them. Second, the deployment and integration of AI technologies into open architecture platforms like the F-35 is easier and faster than deploying them on, say, the F-16 – an aircraft that was not designed to operate in a digital environment. The US will continue to operate a mix of new and legacy systems and face inter-generational and interoperability challenges in deploying AI-enabled capabilities. Third, the rapid proliferation of AI projects is not in itself a measure of success. Bringing AI-enabled capabilities across the 'valley of death' (the transition from development to acquisition), scaling them into wide deployment, and making the necessary organisational adaptations is the more difficult challenge.

The US will continue to operate a mix of new and legacy systems and face inter-generational and interoperability challenges in deploying AI-enabled capabilities.

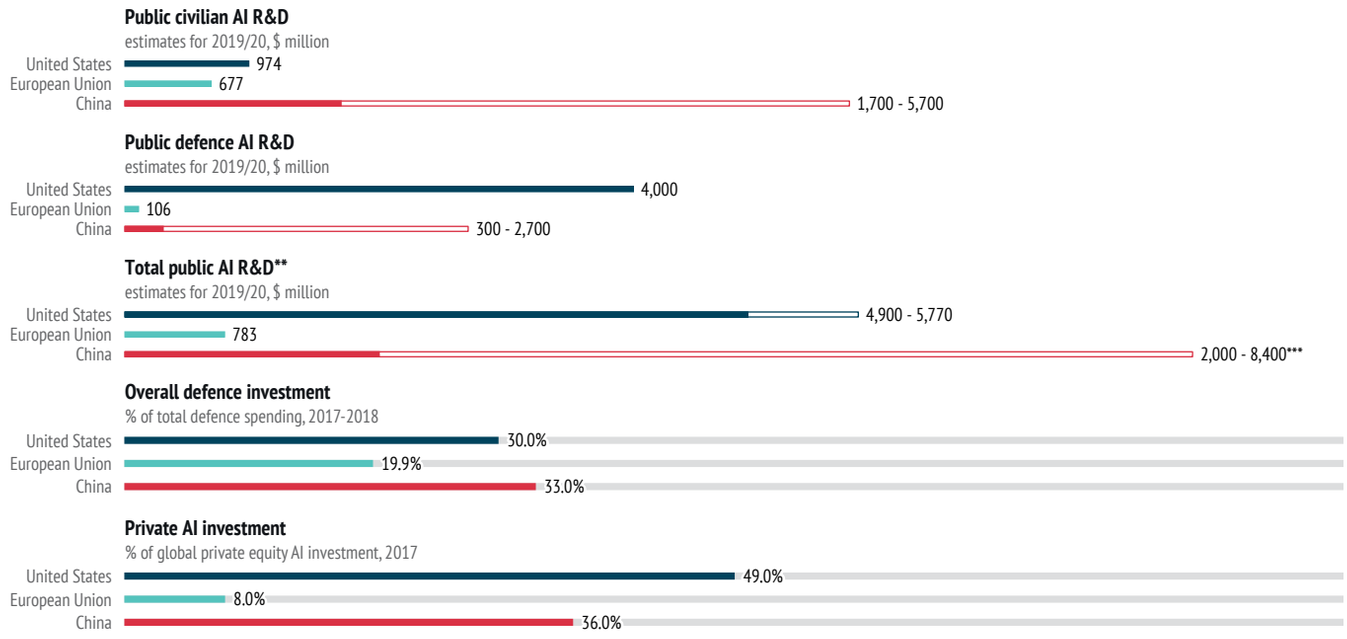
A recent study concluded that the DOD should re-evaluate its optimistically short AI capability development cycles. Quoting the study at length is instructive for its relevance in both the American and European contexts: '… it is important for DoD to maintain realistic expectations for both performance and timelines in going from demonstrations of the art of the possible to deployment at scale in a DoD environment. Careful investments in mission-support and operational AI use cases need to start now, but with the expectation that they might lead to products only in the middle to long term [5-15 years]. Moreover, these investments should be supplemented by appropriate investments in infrastructure and enablers.'[14] A solid framework for testing, verification, validation and certification of AI-enabled capabilities will also be important, in the US and in Europe.

Hard choices between readiness and modernisation

The dilemma around AI defence investment is less about whether it should favour readiness or modernisation and more about the delicate act of finding the right balance between them. Readiness refers to the ability of military units and their equipment to engage in combat as per their intended tasks and in a timely manner. Defence modernisation implies an upgrade of existing capabilities and technologies, including the development of new doctrines and operational concepts. In short, modernisation implies readiness, and both rely on investment in R&D.

The AI investment gap

Comparative AI spending by the United States, China and the European Union (excluding spending by individual EU member states)



* Figures indicate estimated annual spending. Even if EU MS contributions were included, the total figure for the EU would still significantly lag behind the US and China.

** Figures for the US include spending on AI and machine learning technologies, whereas figures for China and the EU represent spending for AI technologies and automation.

*** According to CSET Issue Brief (Dec 2019), there is a very low probability that China spends up to $8,400 million on public AI R&D.

Data: White House, 2019; European Commission, 2019; European Defence Agency, 2019; OECD, 2019, Bloomberg 2019; CSET 2019; McKinsey, 2019

Extensive criticism levelled at the Trump administration for continuing to prioritise readiness and force size over modernisation[15] suggests that Washington has not yet found the right balance between the two. Defense Secretary Esper is proposing an aggressive DOD reform plan to curtail legacy programmes and retire ageing platforms in order to channel funds towards modernisation.[16] The extent to which AI can be deployed in search of cost savings in the DOD is staggering. If extended to the entire Air Force aircraft fleet, predictive maintenance alone would save an estimated $3-5 billion annually.[17] However, the success of Secretary Esper's ambitious reform plan remains uncertain. Expected military services and legislative pushback aside, the 2021 budget could shift because of the November presidential elections. Operational needs in the Middle East and in Europe could also tilt the balance towards procurement and freed funds could still prove insufficient to compete against China and Russia if they are not channelled into R&D.

IMPLICATIONS FOR EUROPEAN SECURITY AND THE TRANSATLANTIC PARTNERSHIP

The DoD AI Strategy acknowledges the unique strategic role played by US allies and partners: 'Foreign allies and partners offer critical perspectives and talent that can be leveraged through personnel exchanges, combined portfolio planning, and the deepened interoperability and trust that comes from collaborative AI development and deployment.'[18] However, the strategy's unclassified summary does not mention NATO or the European allies at all. The focus on interoperability is certainly welcome, but little is said about the unique challenges it entails and how the DOD plans to maintain transatlantic interoperability. Furthermore, American accusations of European free riding on defence spending, European 'techno-Gaullism',[19] defence market protectionism, Europe's concerns over long-term US commitment to NATO, resentment of Trumpian unilateralism,

and the fear of losing competitiveness in the digital economy, all fuelled by the Twitter politics of the day, have been successful in muddying the waters of transatlantic defence cooperation on AI.

Erosion of transatlantic military interoperability and deterrence?

Despite the ongoing debate in Europe around strategic and technological sovereignty, Europeans continue to have a strong interest in cooperating with the US on defence modernisation. A level of military interoperability between transatlantic armed forces is one prerequisite for continued American strategic commitment to European defence. The transatlantic partners already enjoy a solid foundation for interoperability through NATO and the Alliance is actively adapting its interoperability standards and metrics to account for AI.[20] Understandably, this lends strategic scope to transatlantic AI investment, and gives rise to concerns about technological and capability gaps and the erosion of transatlantic military interoperability. It also puts pressure on European states to be fast followers of US defence modernisation efforts, through either technological and operational imitation or off-the-shelf defence purchases. The choice is either that, or fall behind, with all the negative security implications that the latter option entails.

There is a growing transatlantic digital gap, including on AI,[21] that feeds into broader concerns around transatlantic military interoperability. Europe is already behind in the global technological competition on AI, including in R&D and technology adoption. The EU, the world's second-largest economy, only attracts 8% of global private equity AI investment, most of which goes to the United Kingdom,[22] now outside the Union. In a demonstration of the flattening effects of AI, a post-Brexit EU might attract as little AI private funding as Israel – approximately 4% of the global total. Diffusion of digital technologies in Europe remains slow and AI is mostly a niche market for European companies. The European Commission's pledge to spend €20 billion a year for the next decade to support AI R&D, together with national European pledges, will help narrow the AI investment gap with the US and China. It may not close the gap, but it will undoubtedly make Europeans more competitive.

European states are also increasing their defence spending, which means more funding will be redirected towards R&D and emerging and disruptive technologies. Nevertheless, Europe is lagging significantly behind the US and China on defence AI R&D. Of course, European defence R&D has traditionally been lower than the US and the transatlantic technology gap is an enduring feature of the relationship. At €44.5 billion, European defence investment is not negligible, but defence research is still decreasing, begging the question whether this state of affairs is sustainable. The fact that 90% of European defence AI R&D comes from 7 out of 27 countries highlights the intra-European technological divide between the AI haves and have-nots. While national AI efforts and limited bilateral cooperation may help narrow the investment and technological gaps between Washington and leading European AI champions, it will not close a structural security vulnerability for the Union and for the transatlantic partnership, with negative impact on interoperability.

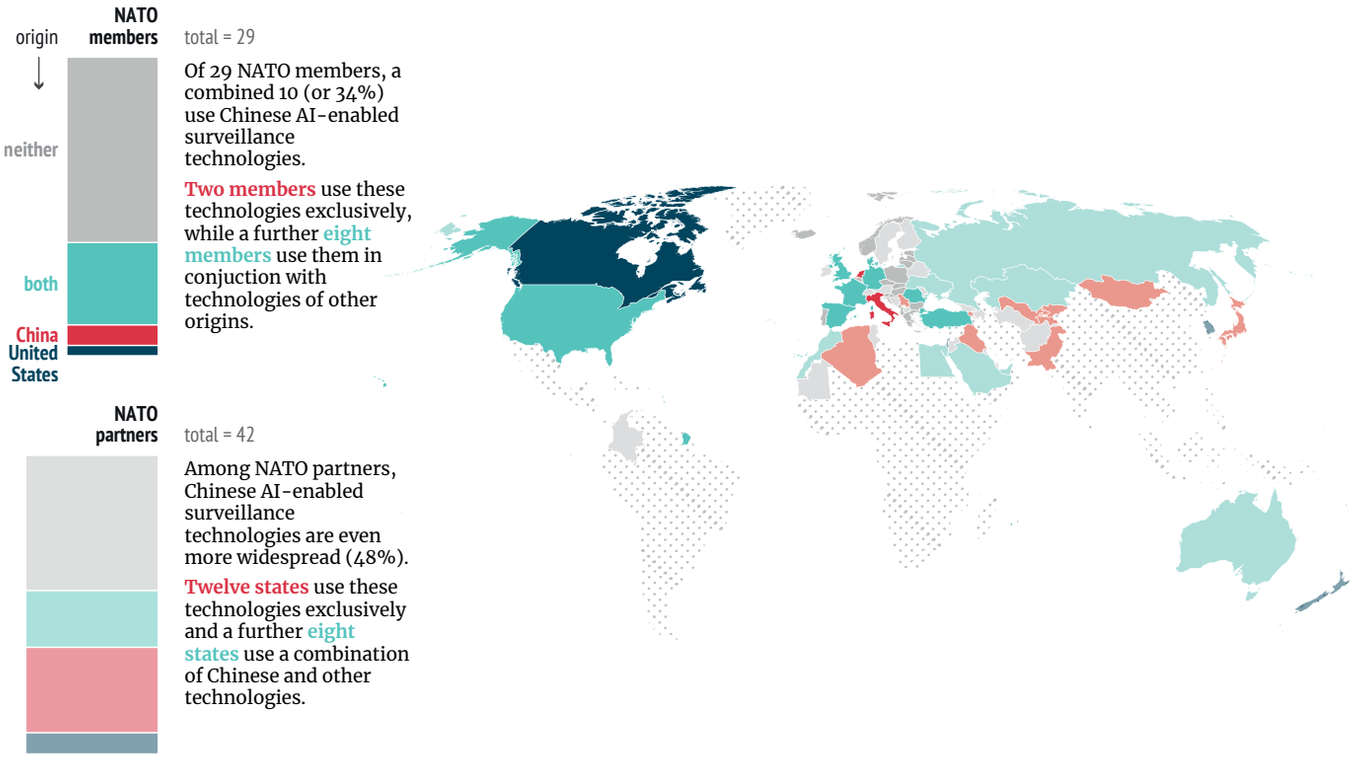
EU funds are now available through the European Defence Fund (EDF) to enable European risk sharing and to complement European national defence R&D budgets. Notwithstanding uncertainty about the EDF's final budget, such efforts will only yield results if backed by a common European vision on the role of AI in defence. This needs to be enabled by a strategic and well-funded plan with clear progress metrics and time horizons. While American AI-enabled capability programmes currently run under two years, Permanent Structured Cooperation (PESCO) projects that focus on developing AI-enabled capabilities, of which there are few, have no delivery deadline attached. Developing a view of the digitalisation of European armed forces appears to be an incremental process and acquiring the AI-enabled capabilities discussed in the previous section could be a 10-year challenge. In contrast, in 2021, the US Army is planning to start piloting the Army's Multi-Domain Operations concept in Europe[23] and the Air Force is experimenting with capabilities to enhance its ability to network and exchange data between US capabilities and those of its allies and partners.[24]

European states are not only under pressure to maintain technological superiority against possible enemies, but also to keep up with US developments on AI. Maintaining interoperability implies a transatlantic agility test on AI-enabled capability development and on avoiding fragmentation in the pursuit of rapid adoption of AI. While it is safe to assume that the US deployment of AI-enabled capabilities – driven by developments in Chinese use of military AI – will accelerate at a faster pace than European initiatives in this domain, Europeans have incentives to be fast adopters of AI to optimise their operational performance. Europeans have less legacy software to replace and more ongoing capability development to deploy built-in AI solutions. This means they have an opportunity to use AI to leapfrog forward in operational readiness and effectiveness.

Nevertheless, the costs of closing the digital technological and capability gaps are mounting for Europe. One estimate places these costs at $30-50 billion every year for a decade.[25] In other words, the digital modernisation of European armed forces comes with a very high price tag. This amount is higher than the

AI-enabled surveillance technologies

Smart cities, facial recognition and smart policing technologies deployed by NATO members and partners, and their origin



Data: Carnegie Endowment for International Peace, 2019; NATO, 2019

entire collective annual defence R&D spending of EU members and it would be very difficult to sustain. Moreover, European defence budgets are subject to more pressures and constraints than the American defence budget. European states are still focused on the expensive undertaking of closing enduring and costly capability shortfalls and ensuring European military capabilities are ready for deployment – both of which are necessary for increasing their ability to act autonomously. Progress in this area is critical for Europe. It will also help to answer American calls for European troop and equipment contributions to joint operations. However, this does not mean Europeans will be successful in appeasing Washington's continued pressure on them to accelerate defence-spending increases, shift more funds to R&D, and buy more American weapons.

Certainly, there are security gains from US deployment of AI-enabled capabilities in Europe. These include enhanced situational awareness, more secure and survivable command, control and communications (C3) systems in A2/AD environments, resilient logistics, and increased mobility of smaller units, such as those in the NATO enhanced forward presence. In the face of persistent calls in Washington to bring troops back home, rebalance to Asia, and save defence dollars, these same AI-enabled capabilities could also shift US perceptions of the size and structure of its military footprint in Europe. If AI-enabled capabilities make smaller military units like battalions more ready, defendable, stealthy, manoeuvrable and sustainable in enemy territory and in A2/AD areas, then a large military footprint will be strategically and financially untenable.

Such changes go to the core of perceptions about US (extended) deterrence and reassurance in Europe. The European Deterrence Initiative (EDI) relies on a rotational but continuous military presence in Europe, pre-positioned military equipment and a heavy schedule of joint exercises with European allies and partners. This is intended to deter Russia and to reassure allies and partners of US commitment to their defence. However, it is arguable whether automated warehouse management of pre-positioned American equipment, or indeed the rotational deployment of automated capabilities, will be as reassuring to allies as American boots on the ground. Deterring Russia will continue to rely on physical tripwires in the Baltics and maritime presence in the Black and Baltic seas and in the North Atlantic. The interplay between US military presence and deployment of AI-enabled capabilities in Europe will affect deterrence in ways we do not yet fully understand.[26] With virtually every European ally expecting the US to defend them against a Russian attack,[27] the answer to these issues is paramount for the future deterrence and defence strategy of the transatlantic alliance.

Relatedly, NATO will be increasingly challenged to maintain interoperability and ensure politically relevant contributions, particularly from smaller allies without advanced AI-enabled capabilities. This is because the transatlantic allies operate a mix of new and legacy systems that are diverse and produce data that is fragmented and heterogeneous. Indeed, a replay of the experience in cyber capabilities is entirely possible in AI: a small number of transatlantic partners deploy advanced AI-enabled systems to maintain their full-spectrum military capabilities and the rest either eventually adopt a variety of less sophisticated AI capabilities to remain relatively interoperable or develop AI niche capabilities to enhance their added value to the alliance. This would increase the intra-alliance AI dependence on nations with full-spectrum AI-enabled capabilities, including in the areas of collective decision-making, operations, collaborative capability development and counter-AI.

This asymmetry is particularly worrisome for rapid decision-making in NATO, one of the pillars of the Alliance's adaptation efforts. Wider information asymmetry between transatlantic partners underpinned by asymmetry in AI-enabled capabilities could hinder rapid decision-making between the allies.[28] Such dynamics fuel American unilateralism and exacerbate long-standing tensions between the transatlantic partners, as recently demonstrated by the American withdrawal from Syria and the killing of Iranian general Qassem Soleimani. Consequently, European partners will face important ethical, legal and strategic considerations about US operational use of AI-enabled capabilities in Europe and will have to manage the increased risks of European entanglement in an unintended US conflict. This will be a far cry from Europe's attempt to take back control of its own defence. For these and other reasons, it is difficult to overestimate the importance of active European participation in the formulation of rules for the operational use of AI.

The EU-NATO framework: between a hard rock and digital divide

Data shows a growing diffusion of security-sensitive Chinese AI technologies among NATO members and partners. This is a new challenge for NATO and the EU alike. The recent Turkish decision to buy the Russian S-400 air defence system and the persistence of Soviet-era equipment in the arsenals of several allies aside, during and after the Cold War NATO member states did not use Soviet or Russian security technology to a comparable degree. 34% of NATO members and 48% of NATO partners are using Chinese AI-enabled surveillance technology and there is an emerging trend among them to deploy both US and Chinese AI technologies at the same time. This picture is further complicated by the transatlantic debate on Chinese participation in building European 5G networks. On 5G, political fragmentation and uncompromising national positions have prevented broader cooperation on tackling the Chinese challenge. These examples highlight three emerging transatlantic differences on AI, data and digital governance issues, and diverging perceptions of the threat posed by China, which the EU-NATO framework may be expected to manage.

First, the versatile nature of AI technologies may mean that European states can be fast followers in the digitalisation of defence. Because AI uses go well beyond the military realm, AI governance is not the exclusive responsibility of the transatlantic alliance. Indeed, much depends on the Union and its ongoing efforts to frame and regulate AI technologies, set industrial standards and ethical principles for their use, and establish a data governance structure that enables the development and lawful use of AI. This means that the deployment of AI in military applications falls in the framework of EU-NATO cooperation.

The trouble is that Europeans have a different perspective on AI than Washington.[29] Perhaps with the exception of France,[30] Europeans view AI primarily through a geo-economic lens – as directly connected to their economic competitiveness. Many in Europe feel that, if left unaddressed, the European digital and AI technology gap will transform Europe into a 'digital colony'.[31] Reinforced by the White House's transactional approach, by European concerns over their own competitiveness in the digital economy, and by Brussels' fears of being pushed to the margins of US-China AI competition, there are pressing calls for Europe to defend its 'digital sovereignty.'[32] Others believe Europe has a strategic opportunity to advocate a veritable 'third way' on AI.[33] The European Commission's 'digital package' (released on 19 February) arguably goes a long way in this direction.

Second, this suggests that a significant structural shift in the partnership is emerging. As President Macron has argued, the challenge in this technological competition is tied to sovereignty: 'The battle we're fighting [on AI] is one of sovereignty … If we don't build our own champions in all new areas – digital, artificial intelligence – our choices… will be dictated by others.'[34] The implication is that Europe's digital vulnerability is becoming a geopolitical security problem, reinforced by pre-existing European dependencies, not least in defence. The expectation is that the US should help its European partners remain strategically relevant in the arena of great power competition in the new digital era.

Lastly, there is the issue of assessing the threat represented by AI defence technologies. Here, too, transatlantic positions diverge. The US AI Strategy is clearly driven by the threat posed by China and, to

a lesser extent Russia. China has announced its ambition to be the global leader in emerging technologies by 2030 and pledged $150 billion investment in AI technologies.[35] Not only is digital modernisation a strategic must for US military superiority and the preservation of the international order, but, unlike the Europeans, the US perceives a rapidly closing window of opportunity to achieve it before China reaches strategic parity.

Washington is already locked into a strategic competition with Beijing and expects to leverage its enduring and strong European alliances and partnerships to its advantage.[36] Fuelled by the Department of Commerce and the White House's insistence on increasing restrictions on technological exports and by the recent Chinese decision to replace all foreign computer equipment and software within three years,[37] the debate about a US-Chinese technological decoupling is unnerving European audiences. This is not to say Europeans are not concerned with Chinese actions and presence in Europe. Europeans see China as a systemic rival, particularly in the geo-economic field, but limited European capabilities to project military power into the Indo-Pacific translate into a marginal security role for Europe in the region. NATO, too, has recently reflected on the security challenges created by Chinese presence in Europe. However, neither the EU not NATO are prepared to call China a threat. As already demonstrated by the 5G debate, European allies and partners are increasingly concerned about being caught in the middle of or being negatively impacted by the perceived zero-sum dynamics of the strategic confrontation between Washington and Beijing.

Political problems surrounding the framework aside, EU-NATO cooperation will come under increasing pressure in the years to come. The challenge ahead is twofold: Europeans need a strategy for military innovation, including AI, underpinned by political will, sustainable funding and broader R&D cooperation. And the transatlantic partners need to design a common AI governance approach with clear interoperability metrics, standards and ethical considerations. Only then will they be able to deliver a digital bridge between North America, the UK and Europe and avoid a deepening transatlantic digital divide.

References

1 Department of Defense, *Summary of the 2018 DOD Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*, February 2019, p. 4-5.

2 Defense Innovation Board, *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*, October 2019.

3 Department of Defense, Joint Chiefs of Staff, *Joint Doctrine Note 1-19: Competition Continuum*, June 3, 2019, p. 5.

4 Patrick Tucker, "War on Autopilot? It Will Be Harder Than the Pentagon Thinks", *Defense One*, February 12, 2020.

5 Andrew Feickert, "Defense Primer: Army Multi-Domain Operations (MDO)", *Congressional Research Reports*, IF11409, January16, 2020.

6 U.S. Joint Staff, *Description of the 2018 National Military Strategy*, 2018, p. 3.

7 Nathan Strout, "A Pentagon experiment to process the torrent of data from space", *C4ISR*, September 26, 2019.

8 Sydney J. Freedberg Jr, "Fix It Before It Breaks: SOCOM, JAIC Pioneer Predictive Maintenance AI", *Breaking Defense*, February 19, 2019.

9 Elias Groll, "The Pentagon's AI Chief Prepares for Battle", *Wired*, December 18, 2019.

10 Luke Hartig and Kendall Vanhoose, "Solving One of the Hardest Problems of Military AI: Trust", *Defense One*, April 1, 2019.

11 Loren DeJonge Schulman *et.al*, "The Rocky Relationship between Washington and Silicon Valley: Clearing the Path to Improved Collaboration", *CNAS* Report, July 19, 2017.

12 Scott Shane, Karen Weise and David E. Sanger, "Pentagon Delays Award of $10 Billion Cloud Computing Contract", *New York Times*, July 31, 2019; Patrick Tucker, "3-Star General: Tomorrow's Troops Need Controversial JEDI Cloud", *Defense One*, August 10, 2019.

13 Defence Innovation Board, "Defense Innovation Board Metrics for Software Development", *SWAP Study Concept Paper*, May 3, 2019, p. S82.

14 Danielle C. Tarraf *et al*., "The Department of Defence Posture on Artificial Intelligence", *RAND Corporation*, December 2019.

15 Eric Edelman and Gary Roughead (Co-Chairs), "Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission", US Congress, November 2018.

16 Mackenzie Eaglen, "Esper Is Attempting the Biggest Defense Reform in a Generation", *Defense One*, January 15, 2020.

17 Defence Innovation Unit (DIU), *Annual Report 2018*, p. 8.

18 Op. Cit., *Summary of the 2018 DoD Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*, p. 12.

19 Tyson Barker, "Europe Can't Win the Tech War It Just Started: The European Union is running in circles in pursuit of digital sovereignty", *Foreign Policy*, January 16, 2020.

20 Carlo Munoz, "Pentagon, NATO to ink long-term MOU for digital modernisation", *Jane's Defence*, December 17, 2019.

21 McKinsey Global Institute, "Notes from the AI Frontier: Tackling Europe's Gap in Digital and AI", *Discussion Paper*, February 2019, p 8.

22 OECD, "Private Equity Investment in Artificial Intelligence", December 2018.

23 Sean Kimmons, "Army to build three Multi-Domain Task Forces using lessons from pilot", US Army News Service, October 11, 2019.

24 Valerie Insinna, "Sorry, Sierra Nevada Corp. and Textron: The US Air Force isn't buying light attack planes", *Defence News*, February 11, 2020.

25 Munich Security Conference, "More European, More Connected and More Capable: Building the European Armed Forces of the Future", 2017, pp. 23-24.

26 Yuna Huh Wong *et.al*, "Deterrence in the Age of Thinking Machines", *RAND Corporation*, January 2020.

27 Moira Fagan and Jacob Poushter, "NATO Seen Favorably Across Member States", PEW Research Center, February 9, 2020.

28 Tomas Valášek, "How Artificial Intelligence Could Disrupt Alliances", Carnegie Europe, August 31, 2017.

29 European Commission, "White Paper on Artificial Intelligence - A European approach to excellence and trust" COM(2020) 65 final, February 19, 2020.

30 Ulrike Franke, "Not Smart Enough: The Poverty of European Military Thinking on Artificial Intelligence", ECFR, December 2019.

31 Julien Nocetti, "Will Europe remain a 'digital colony'?", in Thomas Gomart and Marc Hecker (eds), *European Elections 2019: Structuring the Debate*, Études de l'Ifri, February 2019.

32 Guy Chazan, "Angela Merkel urges EU to seize control of data from US tech titans", *Financial Times*, November 12, 2019.

33 John Thornhill, "There is a 'third way' for Europe to navigate the digital world", *Financial Times*, February 19, 2019.

34 "Macron throws €5 billion at digital start-ups", *RFI*, September 18, 2019.

35 State Council of China, *New Generation Artificial Intelligence Development Plan*, July 2017.

36 Gideon Rachman, "Why Europe will choose the US over China", *Financial Times*, December 9, 2019.

37 Yuan Yang and Nian Liu, "Beijing orders state offices to replace foreign PCs and software", *Financial Times*, December 8, 2019.

PRINT
ISBN 978-92-9198-867-9 CATALOGUE NUMBER QN-AK-20-003-EN-C ISSN 2599-8943 DOI 10.2815/041848
ONLINE
ISBN 978-92-9198-868-6 CATALOGUE NUMBER QN-AK-20-003-EN-N ISSN 2315-1110 DOI 10.2815/268841