EUROPEAN UNION
Institute for Security Studies

DIGITALISING DEFENCE

BRIEF / 4
Mar 2020

Protecting Europe in the age of quantum computing and the cloud

by

Daniel Fiott
Security and Defence Editor, EUISS

Summary

- Digital technologies can vastly improve the operational readiness, effectiveness and technological sovereignty of Europe's armed forces. For defence to benefit from digitalisation, both the greater interoperability of digital technologies and financial investment is required. The Multi-annual Financial Framework is a test for how serious EU member states are about the digital agenda but low national defence R&D investments are also contributing to an erosion of Europe's digital power.
- Europe does not have enough statistical clarity of the digital state of its armed forces today. A number of 'quick win' initiatives can be undertaken by the EU in the short term. Without overhauling existing initiatives, member states could record progress on their national defence digitalisation efforts through the reporting mechanisms available under the CARD and PESCO.
- Beyond short-term measures, discussions about the digitalisation of defence could be integrated into the forthcoming 'strategic compass'. The Union needs better foresight capacities to understand the link between digital capability development and digital vulnerabilities and how digitalisation should be included in any future European threat analysis and defence strategy.

INTRODUCTION

Any discussion about the digitalisation of defence is hampered by the imprecision of associated terms and words. 'Cyber', 'the cloud', 'Internet of Things' (IoT), 'block chain' and 'quantum computing' are widely used but their exact meaning or application can be quite fuzzy. The truth is that we may be intellectually ill-equipped to understand the full intricacies and implications of digitalisation, even if the economic rationale for digitalisation is clear. In fact, some estimates show that the digitalisation of products and services could add more than €110 billion to industrial revenue in Europe over a relatively short time frame of five years, so it is easy to see why the economic rationale for greater digitalisation is so powerful.[1] Yet digitalisation is clearly not just about economics and the geopolitical ramifications of a proliferation of digital technologies is becoming a mainstay of international politics today.[2] The assumption is that the competition to control new technologies (both hardware and associated software and algorithms), and the willingness to use them to gain an advantage over other states, underlines the growing importance of 'digital power'.[3] It is for this reason that the European Commission has stated that it is imperative for the EU to establish 'technological sovereignty' in areas of key strategic importance such as defence, space, mobile networks (5G and 6G) and quantum computing.[4]

What digitalisation means for defence is perhaps even more unclear. While the process has accelerated since the 1970s, and armed forces are no strangers to the need to adapt to and integrate new informatics systems and processes, the modernisation and digitalisation of Europe's armed forces is essential. Without the technological command of digital technologies, Europe could lose international influence and political autonomy.[5] In this respect, the fact that the continent is projected to need to spend $120-$140 billion on the modernisation and digitalisation of its armed forces in the coming years (or $20-$30 billion annually) is a daunting and pressing challenge.[6] Indeed, this very issue was the focus of a May 2019 food for thought paper published by Finland, Estonia, France, Germany and the Netherlands. These countries implied that Europe's militaries cannot fully function in an information dense operational environment where actors who can effectively harness computing, Artificial Intelligence (AI) and data are likely to have a military advantage.[7]

In addition to this member state-backed food for thought paper, the European Commission released its long awaited 'digital package' on 19 February 2020, detailing how Europe could reap the benefits of AI, computing power and data spaces while simultaneously managing the risks of these technologies. The Communications on 'shaping Europe's digital future' and a 'European data strategy', plus the white paper on AI, do not really mention defence.[8] With the 10 March release of the new EU Industrial Strategy, however, synergies between civil and defence technologies will be further explored.[9] Even though the European Defence Agency (EDA) is already studying the ramifications of digitalisation for defence, this broader industrial approach by the Commission is understandable given the wider relevance of digitalisation to European society. Nevertheless, these initiatives do beg two interrelated questions: 1) how might digitalisation affect the way Europe's armed forces plan and act? and 2) what should defence planners[10] in Europe do to benefit from digitalisation while also managing the inevitable risks?

This Brief answers these questions with a view to filling a gap in the EU's understanding of how digitalisation could affect Europe's armed forces and wider defence. To this end, the Brief is structured in three parts. In part one it looks at the meaning of digitalisation and existing initiatives in the defence sector. Part two will then uncover the limits of digitalisation in defence. Finally, part three will focus on the specific challenges of digitalisation in defence and it asks whether the EU can assist member states and armed forces in overcoming them. Accordingly, the Brief not only seeks to demystify discussions about the digitalisation of defence but it also volunteers some policy options.

BYTES, SWEAT AND TEARS

Discussions about digitalisation can be blighted by a lack of definitional clarity. We must first distinguish between *digitisation* and *digitalisation*. The former refers to the basic process of converting analogue data and information into bytes or lines of binary code (e.g. transforming an old printed photograph into a JPEG file). Digitisation allows computers to process, communicate and store information more flexibly and efficiently. The latter, however, is the term given to collective technological advances in computing power, data collection, processing and storage and networking between computer devices. Digitalisation is therefore a transformational process that may alter how Europeans live and how they plan for future wars and conflict.

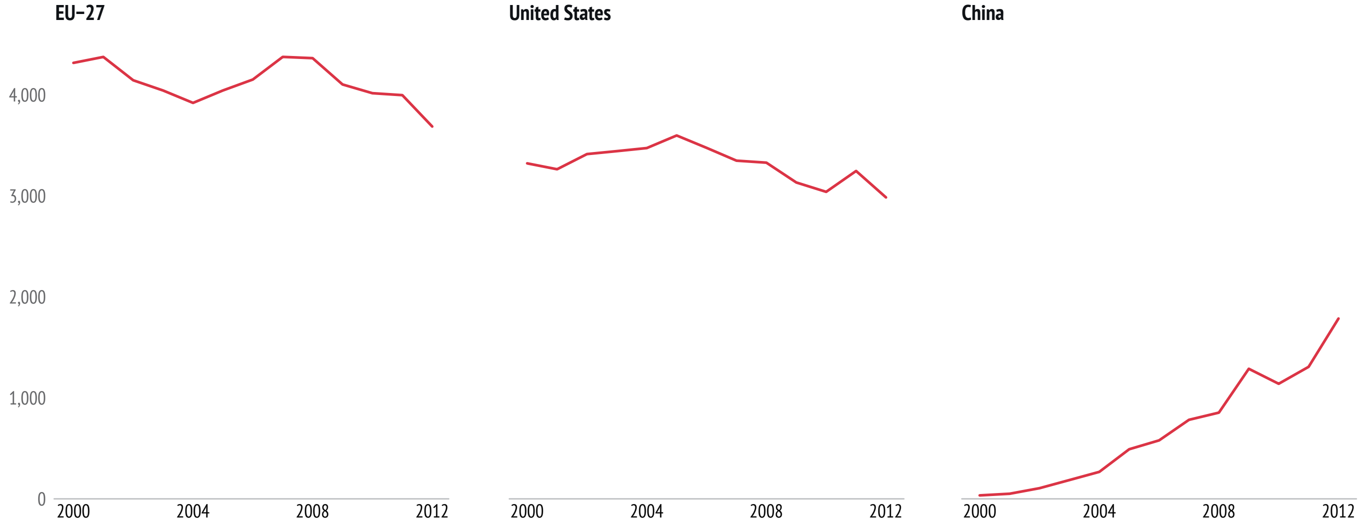
Digitalisation is a transformational process that may alter how Europeans live and how they plan for future wars and conflict.

Armed forces in Europe are more than familiar with digitisation and digitalisation as they have long used computers to manage logistics and supply inventories, wage payments and the maintenance of personnel records. Military intelligence has also long profited from computer technology (e.g. Turing and Welchman's Enigma decryption computers in the 1940s) and since the 1960s armies have used computers to perform complex mathematical calculations for artillery and ballistics accuracy.[11] With the invention of the microprocessor in the 1970s, militaries steadily began to use computers for command and control (C2) and intelligence, surveillance and reconnaissance (ISR). In the 1990s, rapidly increasing computing power and masses of data were used to improve battlefield communication between units and strategic command and to enhance precision-strike capabilities (this was called the Revolution in Military Affairs (RMA)).

Military communications, sensoring, logistics and maintenance and C2 are almost fully computerised and interconnected today, so cyber defence has become a vital element of enhancing the digital resilience of Europe's armed forces. As military equipment, processes and informatics systems become increasingly intertwined, the potential for cyberattacks increases. Experiences such as the 'Conficker' worm that infected French naval systems in 2009, and which led to the

Patents granted in the ICT sector

Issued by the European Patent Office, 2000–2012



Data: OECD Science Technology and Industry Outlook, 2019

grounding of Rafale jet fighters, clearly need to be avoided.[12] On the back of such experiences, France has pledged €1.6 billion up to 2025 for its cyber defence,[13] but a number of other EU member states and NATO allies have also created Joint Cyber Commands, invested in cyber defence research (e.g. the Netherlands is investing €6.5 million per year)[14] and/or have established cyber exercises and training centres (e.g. Estonia created its centre in April 2019).[15]

Most European militaries and defence ministries recognise that international cooperation is vital to their 'digital defences'. Within NATO, European countries are working towards the Cyber Defence Pledge agreed in July 2016 to enhance allies' cyber capacities and the alliance has set up Cyber Rapid Reaction Teams and a Cyberspace Operations Centre. In the EU, there are presently four specific cyber-related projects under Permanent Structured Cooperation (PESCO) and the European Commission will be making available €17.7 million for cyber situational awareness and defence capability investments under the European Defence Industrial Development Programme (EDIDP) in 2020. As part of the Union's wider Cyber Defence Policy Framework (CDPF) and Capability Development Plan (CDP), cyber- and digital-related concerns are addressed including cyber capability development, training and exercises, the protection of Common Security and Defence Policy (CSDP) communication and information systems and more. Bodies such as the EU Military Staff (EUMS) are subsequently working on initiatives such as integrating cyber defence training into the EU Battlegroup certification process.[16] Further still, since February 2016 NATO and the EU have been implementing a technical arrangement on cyber defence with a view to exchanging information on cyber emergency responses.

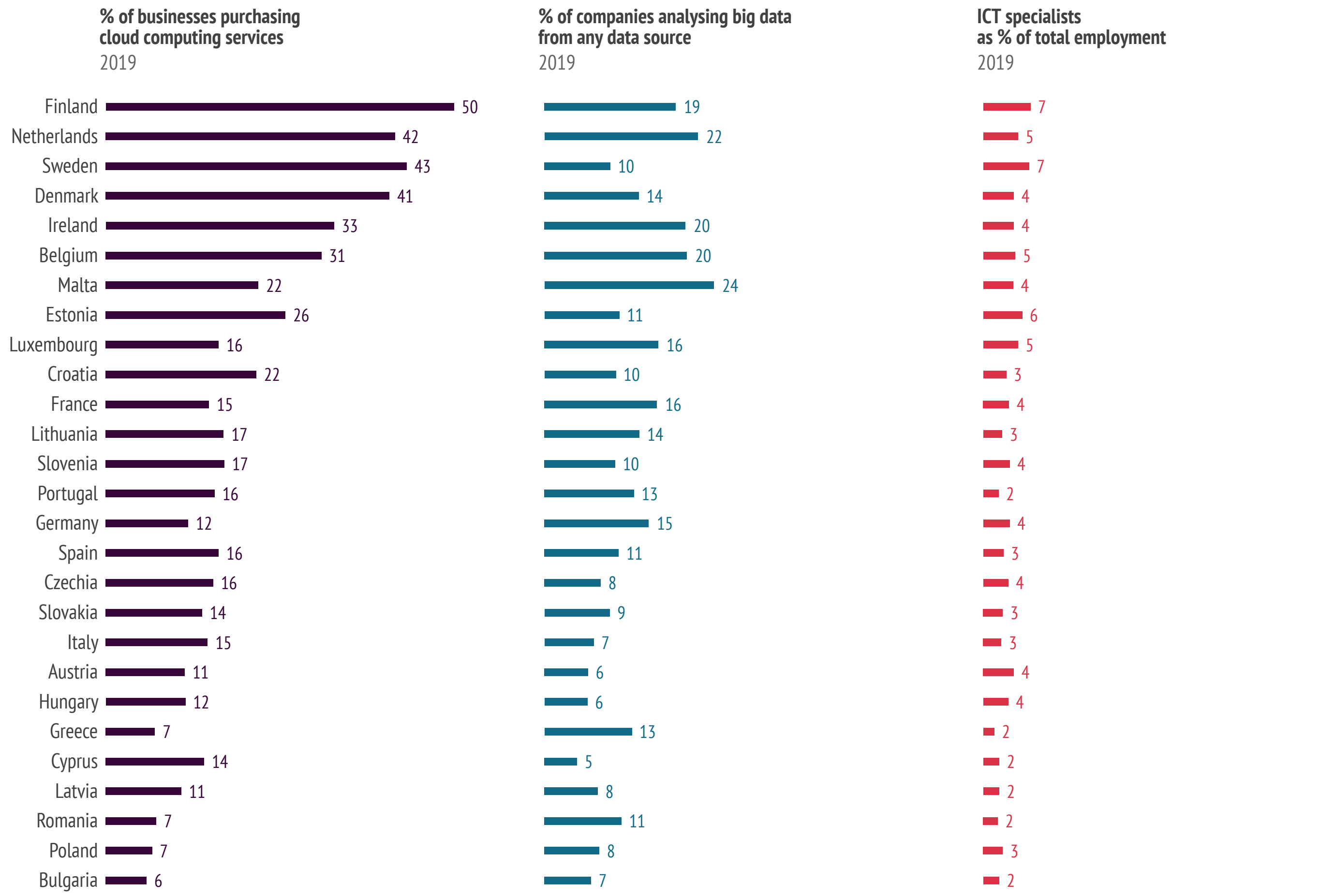
Given the range of initiatives already in place, one might be forgiven for thinking that EU member states and institutions have already designed the 'code' needed to help Europe's armed forces transition to the digital age. However, digitalisation confronts defence ministries and armed forces with unique challenges and questions. First, advances in the cloud, IoT, block chain and quantum computing may have unintended and/or unexpected consequences for the performance of military equipment and capabilities, as well as how defence planners design and conduct operations. Second, the use of digital technologies for defence may presuppose changes in military doctrine or challenge the way military hierarchies and defence bureaucracies have traditionally functioned. Despite the fact that defence firms are producing new digital technological solutions for warfare, defence planners are not entirely sure how – if at all – digitalisation will alter the character of warfare.

HEAD IN THE CLOUD: PUTTING DIGITALISATION IN PERSPECTIVE

Whether technology can ever really fundamentally alter the character of warfare is a well-established debate in scholarly circles. Some would argue that computing power, AI and the wide use of data do little to fundamentally address political sensitivities that run through debates related to capability development, force generation and the use of military force. In this sense, digitalisation should not be seen as some silver bullet for every problem

Digital uptake in the EU

Ranking of member states in three ITC-related categories



% of businesses purchasing cloud computing services 2019

% of companies analysing big data from any data source 2019

ICT specialists as % of total employment 2019

Data: European Commission - Digital Scoreboard, 2020; Eurostat, 2019 and 2020

facing Europe's militaries and a human dimension will be required for politico-strategic guidance and maintaining the morale of troops, amongst other things. Not overly investing in the hype surrounding technology has been a mainstay of military-theoretical discussions. After the US' rapid victory over the Iraqi military in the early 1990s, for example, some scholars and policymakers lauded the idea that technological mastery in the Global Positioning System (GPS), digital communications, electronic warfare, stealth, satellites and precision-strikes could lead to military superiority.[17] It became apparent after the US intervention of Afghanistan in 2001, however, that technology could only take US forces so far when counter-insurgency strategies were required instead.

Based on such experiences, there is a fear that digitalisation could be used as a technological 'sticking plaster' to deal with intractable politico-strategic problems in warfare. Take data management, for example. European militaries already handle vast amounts of data and they process and use data for logistics, equipment maintenance, personnel health, cost management and locating specific skills and talent (e.g. languages, special training). However, having centrally accessible data sources that can be used rapidly by military leaders across all branches and services is a challenge. While advances in AI are being touted as a means to deal more effectively with data management in the military, research shows that data management processes in the military are still subject to inter-service rivalries (i.e. which branch holds data holds power) and a comprehensive data management system does not do away with the need for military leadership (e.g. should more resources be diverted to high performing battalions or soldiers compared to underperforming ones?).[18]

Perhaps one of the more vivid examples of how human behaviour and digitalisation interacts can be seen in how military personnel use digital technologies. Today's reality is that – just like anybody else – personnel in the armed forces increasingly use social media apps and geo-location services. This comes with a risk. The data and information produced by military personnel using digital technologies may incur a strategic disadvantage. Geo-location services and devices (e.g. smart watches) can hand foreign intelligence services information about where troops are directly based. Additionally, the use of social media to share photos with family members in the pre-deployment phase can be used by intelligence services to ascertain whether a new deployment (especially a covert one) is on its way. Additionally, 'selfies' of personnel in barracks or military installations may inadvertently put sensitive information into the public domain (e.g. computer screens in the background).[19] Of course, we could blame technologies for such vulnerabilities but the reality is that a new behaviour that is more sensitive to the risks that digital technologies potentially entail needs to take root in Europe's militaries.

Finally, there are also limitations to the technologies being lauded as having a disruptive effect on defence. Take quantum computing, for instance. This technological domain is already being touted as the next step forward in computing power, and some studies claim that it could revolutionise naval navigation by replacing GPS with atomic clocks[20] or greatly enhance defensive/offensive cryptography capabilities.[21] Quantum computing is seen as a way to overcome the limitations of classical computing because it breaks the strictures of linear coding. Bits and bytes in classical computing can only be a 0 or a 1 at any one time, but quantum's qubits can be a 0 and 1 at the same time.[22] Theoretically, this allows quantum computing to make many more calculations. Although the calculations are disputed, Google argues that the task that took its 53-qubit computer 200 seconds to make would take the fastest supercomputer on earth (IMB's 'Summit') 10,000 years.[23] Despite these claims, however, quantum computers require cooling devices no smaller than a van and large amounts of energy, plus quantum calculations can result in error at the slightest temperature or electromagnetic change. These are hardly attributes that are conducive to a military environment.

Europe's armed forces have to contend with greater digital connectivity, congestion and uptake.

OK COMPUTER: MANAGING THE RISKS OF DIGITALISATION IN DEFENCE

European militaries should not, however, take any comfort from the uncertainties surrounding the development of digital technologies. The more Europe's militaries become dependent on digital technologies the more they become vulnerable to the inherent risks of greater technological connectivity. The development and application of these in defence will likely result in adversaries having to find new weak points in Europe's digital defences (this has been called the 'capability/vulnerability paradox').[24] For example, looking many decades into the future the use of quantum computing may give Europe a technological edge in areas such as cryptography but it may result in certain vulnerabilities. Although secure quantum communications will also depend on high-quality organisational coordination within governments,[25] and despite the currently low-levels of technological readiness in the domain, advances in quantum communication already promise to greatly diminish the risk of data hacking due to the extreme difficulty involved in tampering with qubits. Of course, in the future it may also be possible to manipulate qubits in order to hack digital systems but the assumption today is that quantum computing may revolutionise communications and cryptography.

On the face of it then, quantum computing could be an advantage for military services but there are also potential risks. If it is assumed that quantum communication will greatly reduce the risk of remote hacking, then physical infrastructure may become more of a target for military actors – quantum communications would still rely on physical infrastructure. 'Quantum links' are already being developed today and China has established an almost 2,000 km land-based quantum link between Beijing and Shanghai. Such a feature of the digital age is likely decades away for most countries, of course. In addition, critical infrastructure protection requires by its very nature close cooperation between military actors and civilian bodies and private actors – so a solely military solution to the protection of Europe's quantum infrastructure is unrealistic. Nevertheless, we should ask whether comparable future quantum links on the European mainland would be considered military targets by potential adversaries, and, if so, we should think about how we would protect them and other digital infrastructures.

As far-fetched as this example may seem, it highlights the need for European policymakers and defence planners to develop an effective Critical Infrastructure Protection (CIP) strategy that deals with the false dichotomy between 'virtual' and 'physical' infrastructure. Given that the European Commission plans to release its proposal for additional measures on the CIP Directive (2008/114/EC) at the end of 2020, there could be a mutual opportunity for policymakers and defence planners to better understand the military aspects of CIP, especially with regard to digital infrastructure. Defence planners already have experience with CIP, as can be seen by military strategies to protect the global web of undersea cables that sustain the Internet and digital networks. While fibre optic undersea cables have existed since the late 1980s, defence planners increasingly recognise that damaged energy supply lines and/or undersea cables can disrupt military communications, potentially knocking out C2 networks and strategic weapons systems plus early-warning systems.[26] The EU is already developing capabilities for maritime CIP: for example, five PESCO maritime projects specifically address undersea surveillance and protection.[27]

Beyond the need to secure critical infrastructure, Europe's armed forces also have to contend with greater digital connectivity, congestion and uptake. Digital technology is proliferating at ever faster rates. If, as one report claims, it took 50 million people 75 years to use the telephone but only four years for this same amount to use the internet, then the risk that adversaries will beat European militaries to unlocking innovative ways of using digital technologies is potentially high.[28] Of course, cyber defence is one way of managing the risks associated with the proliferation and connectivity of digital technologies, but any lasting solution must go beyond this. One could argue that defence planners need to maintain analogue systems in order to ensure a minimum operational capacity in case of digital 'blackouts' or electromagnetic disruptions. Most military-applicable components like microchips and processes already require a digital-analogue mix for signals and communication and European manufacturers are already producing these types of components with the EU's support.[29] Despite this, there is a strong case for drawing up scenarios to test how Europe's militaries could operate with 'analogue only' technologies in digitally compromised theatres.

Europe cannot become a 'digital power' on the back of under-investment.

With the creation of the European Defence Fund (EDF), and work towards a 'strategic compass' in 2020, there is an opportunity to better understand and exploit defence-relevant disruptive technologies. One could argue that the EU already has this system in place with the CDP and the Commission's work programme planning under the EDF, and indeed these initiatives already flag needs and shortfalls in areas such as cyber defence and information superiority. Bodies like the European Defence Agency (EDA) have also invested time in exploratory studies on how Big Data might affect the defence sector.[30] Moreover, the Agency is developing the Overarching Strategic Research Agenda (OSRA), which could help better link the Research and Technology (R&T) priorities and interests of member states with the digital-enabled capabilities that the EU requires. Commission officials at DG Defence Industry and Space (DG DEFIS) are looking at ways to better coordinate defence research investments with existing civilian research programmes (Horizon Europe). The Commission also dedicated €7.5 million under the Preparatory Action on Defence Research (PADR) for emerging technologies such as quantum technologies in 2019.[31]

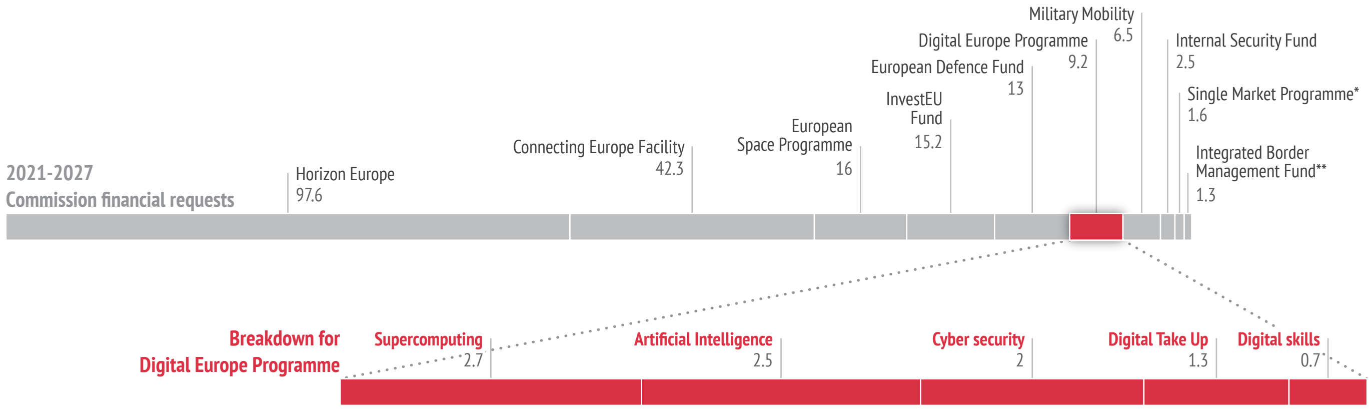
Yet although such efforts are important, there is no EU strategy today designed to understand how Europe's armed forces could use such technologies nor how they would counter their use by adversaries. Thus, what is required is less a systemic identification of capability gaps or disruptive technology areas and more of a continuous scenario-based process that allows defence planners to assess the benefits and risks posed by each digital technology or system. For example, advances in 3D printing, nanotechnologies and digital sensoring have already led to the creation of microelectromechanical systems (MEMS) – or microscopic wireless devices fitted with cameras and sensors that are only the size of a grain of sand. When deployed in their hundreds, these 'smart dust' particles could be used to provide a stealth analysis of a geographical area. Many policymakers and defence planners in Europe would not even know that MEMS exist, let alone have a strategic response to how such technologies could be used or how Europe's militaries would counter them.

Yet defence planners are likely to be increasingly dependent on solutions for 'digital autonomy' outside of the military domain. In reality, any debate about the digitalisation of defence must include a discussion about how defence acquisition processes should adapt to digitalisation. Indeed, there is a debate underway about whether digitally-supported systems such as autonomous weapons could one day replace traditional platforms such as submarines, jet aircraft or aircraft carriers. Furthermore, digitalisation in defence will require sensitive discussions about technological sovereignty and how far Europe's militaries should be dependent on private, non-EU providers for, say, cloud computing. Europe's defence planners need to reflect on whether uploading military-sensitive data to unsecure cloud services is wise, and, as the latest EU strategy on data states, there is a need to ensure that data is not accumulated into large concentrations by any single firm because it could affect market competition and security. In this regard, it is instructive to know that in 2019 US firms held about 70% of the global $96 billion cloud market, with providers from China making up 7%.[32] This 'cloud concentration' could lead to questions about data usage rights and, in the most extreme case, could possibly reduce the military's access to their own information sources.[33]

This is not to say that Europe's armed forces should sit back and wait for industrialists to develop safer digital services, even if these civilian actors have a better knowledge of digital 'state of the art' and 'art of the possible'. For example, it is likely that the issue of digital standardisation and data interoperability will increasingly weigh on European armed forces' abilities to deploy together. The dilemma is three-fold. First, data collection, storage and usage differs between different branches of the military in a number of European states. Second, data usage and sharing between European militaries is under-utilised or even non-existent in many cases. Third, European armed

Financing Europe's digitalisation

Multiannual Financial Framework, € billion, 2021–2027



Data: European Commission, 2018

forces cannot depend on reliable access to data sources developed in the civilian sector (e.g. think of the masses of data generated by border agencies, development agencies or even gendarmerie forces). Although the ability to insure data interoperability will rely on secure technological solutions, Europe's defence ministries and armed forces should reflect on the legal, security and policy processes they would need to develop to manage any future 'European military cloud service'.

DIGITAL POWER EUROPE?

It has been shown that the advances in digital technologies such as quantum computing are not fully understood by the defence sector and Europe needs to be realistic about how these technological advances can benefit EU security and defence. European defence planners and policymakers must acknowledge that digital technologies will create vulnerabilities, as well as opportunities for Europe's armed forces. EU institutions and mechanisms can assist European armed forces' transition to digitalisation, but the reality is that Europe's military bureaucracies need to change from within and digital technologies can only go so far in helping with leadership and decision-making issues. This Brief has shown that there are limits to the benefits of digitalisation in defence, even if the vulnerabilities posed by digital technologies will require defence planners at the national and EU levels to consider what more they can do to improve the resilience of Europe's military computer networks and systems, plus Europe's digital infrastructure more broadly.

There are, however, some immediate (if modest) steps that could be taken by the EU. First, while statistical databases such as Eurostat generate data indicators for digitalisation in the wider EU economy, there is today no concrete data picture for the digitalisation of Europe's armed forces. This is not a call for a publicly accessible database, but digital indicators could form part of the reporting phase of the Coordinated Annual Review on Defence (CARD). Second, even if an 'EU digital military cloud' project would be attractive, there is no need for a specific PESCO project on digital technologies as many already address (if at times only indirectly) digitalisation. There is also no need to open up the 20 PESCO binding commitments to make room for a specific commitment on defence digitalisation because certain commitments already call for operational readiness and interoperability. Instead of projects and commitments, reporting on national defence digitalisation strategies and initiatives in the PESCO National Implementation Plans (NIPs), which ministries of defence submit each year to show how they are meeting the binding commitments, could be encouraged. By filling in the EU's statistical gaps on defence digitalisation, capability shortfalls can be also identified.

The Commission also has to play a role in the digitalisation of European defence. Steps to reduce barriers to data exchanges across EU member states should benefit defence planners, and enhanced digital standardisation could help improve the digital interoperability of Europe's militaries. Yet, in time, the creation of a 'common European defence data space' could capitalise on the Commission's broader civil digital initiatives, as well as address the specific needs of defence. Indeed, the 2020 European strategy for data alludes to nine sectoral 'data spaces' for industry, the Green Deal, mobility, health, finance, energy, agriculture, public administration and skills.[34] These 'data spaces' are supposed to make data management and utilisation easier across the Single Market and so it is not too difficult to see the relevance of such spaces for defence. Notwithstanding the specificities of defence, a 'common defence data space' could be developed to help reduce procurement, equipment and personnel costs across the EU, for instance, and other data spaces could feed this process (e.g. the energy data space could be utilised to reduce the environmental damages caused by defence).

Of course, such policy recommendations can be criticised for proverbially 'beating around the bush'. What is more, they could be accused of adding another layer of reporting obligations under PESCO or naively overlooking the political sensitivities involved in talking about defence and digitalisation in the same breath. This may all be true. However, if Europe's armed forces are not to lose technological ground to adversaries then they need to stay ahead of the digital curve. Today, we hear a lot about the need for Europe to be a geopolitical player that is not only conversant in the language of power but technologically sovereign, too. Yet the gap between rhetoric and reality is far too large. Europe cannot become a 'digital power' on the back of under-investment in national defence Research and development (R&D) or the Multi-annual Financial Framework (MFF), and neither can it really thrive if it is wholly dependent on non-EU digital technologies. Without a strong political and financial commitment to digitalisation and defence, EU member states can only ever hope to be 'digital dwarfs'.

References

[1] European Commission, "Communication on Digitising European Industry: Reaping the Full Benefits of a Digital Single Market", *COM(2016) 180 final*, Brussels, April 19, 2016.

[2] Daniela Schwarzer, "Weaponizing the Economy", *Berlin Policy Journal*, January 6, 2019.

[3] Jean-Christophe Noël, "What is Digital Power?", Études *de l'Ifri*, Paris, November, 2019.

[4] "Questionnaire to the Commissioner-Designate Thierry Breton", 2019, p. 3, https://www.europarl.europa.eu/resources/library/media/20191113RES66410/20191113RES66410.pdf.

[5] European Political Strategy Centre, "Rethinking Strategic Autonomy in the Digital Age", *EPSC Strategic Notes*, Issue 30, July, 2019.

[6] "More European, More Connected and More Capable", joint report by the Munich Security Conference, McKinsey & Company and the Hertie School of Governance, 2017, p. 23.

[7] "Digitalization and Artificial Intelligence in Defence", food for thought paper by Finland, Estonia, France, Germany and the Netherlands, May 17, 2019, https://eu2019.fi/documents/11707387/12748699/Digitalization+and+AI+in+Defence.pdf/151e10fd-c004-c0ca-d86b-07c35b55b9cc/Digitalization+and+AI+in+Defence.pdf.

[8] See: European Commission, "Communication on Shaping Europe's Digital Future", *COM(2020) 67 final*, Brussels, February 19, 2020, p. 5.; European Commission, "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust", *COM(2020) 65 final*, Brussels, February 19, 2020, p. 6.

[9] European Commission, "A New Industrial Strategy for Europe", *COM(2020) 102 final*, Brussels, March 10, 2020.

[10] For the purposes of this brief we employ Breitenbauch and Jakobsson's interpretation of 'defence planning' to include not only decisions about the use of force and military operations but also questions about military leadership, capability development planning, defence spending and strategic foresight. See: Henrik Breitenbauch and André Ken Jakobsson, "Defence Planning as a Strategic Fact: Introduction", *Defence Studies*, vol. 18, no. 3 (2018), pp. 253-261.

[11] Daniel K. Malone, "The Commander and the Computer", *Military Review*, vol. 47, no. 1-6, June 1967, pp. 51-58.

[12] Pascal Brangetto, "National Cyber Security Organisation: France", NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015, p. 11.

[13] NATO, "Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference", Paris, May 15, 2018, https://www.nato.int/cps/en/natohq/opinions_154462.htm.

[14] Ministerie van Defensie, "Defensie Cyber Strategie 2018: Investeren in digitale slagkracht voor Nederland", Den Haag, November 2018, p. 15, https://cyberwar.nl/d/norobots/20181112-Defensie-Cyber-Strategie-2018.pdf.

[15] Estonian Ministry of Defence, "Estonian Ministry of Defence launches Cyber Security Training Centre", April 8, 2019, https://www.kaitseministeerium.ee/en/news/estonian-ministry-defence-launches-cyber-security-training-centre.

[16] Council of the EU, "EU Cyber Defence Policy Framework (2018 Update)", *14413/18*, November 19, 2018, Brussels, p. 11.

[17] See for example Michael J Mazaar, *The Military Technical Revolution: A Structural Framework* (Washington, DC: Center for Strategic and International Studies, 1993).

[18] Calculating military readiness is not a new problem. See for example, John F. Raffensperger and Linus E. Schrage, "A New Paradigm for Measuring Military Readiness", *Military Operations Research*, vol. 3, no. 5 (1997), pp. 21-34.

[19] T.S. Allen and Robert A. Heber Jr., "Where Posting Selfies on Facebook Can Get You Killed: Enemies have targeted U.S. military assets with the help of social media", *Wall Street Journal*, July 26, 2018, https://www.wsj.com/articles/where-posting-selfies-on-facebook-can-get-you-killed-1532642302.

[20] See for example, Ghaya Baili et al., "Quantum-based Metrology for Timing, Navigation and RF Spectrum Analysis", in European Defence Agency, *Quantum Technologies in Optronics: Optronics Workshop Proceedings*, 2019, pp. 60-65.

[21] There remain doubts as to whether 'quantum timing, navigation and sense' can bring any tangible benefit to defence. See: Christophe-Alexandre Paillard and Nick Butler, "Today's Technological Innovations for Tomorrow's Defence", *ARES Policy Paper*, no. 10, December, 2016, fn. 19, p. 20.

[22] By way of an analogy, if classical computing can be likened to a knife (0) and fork (1) where the main task is eating food, then quantum computing can be seen as a Swiss army knife (0 and 1) with the possibility of undertaking multiple tasks simultaneously such as opening a bottle of wine, tightening loose screws or, like cutlery, eating food. After countless minutes of debate, I would like to thank and credit Vasileios Theodosopoulos for this useful analogy. Another popular, if morbid, analogy is Schrödinger's cat where 0 = alive, 1 = dead but in the quantum field the cat can be both alive and dead (0 and 1) at the same time.

[23] Adrian Cho, "IBM Casts Doubt on Google's Claims of Quantum Supremacy", *Science*, October 23, 2019.

[24] Jacquelyn Schneider, "Digitally-Enabled Warfare: The Capability-Vulnerability Paradox", Center for a New American Security report, August, 2016, p. 4.

[25] Jon R. Lindsay, "Demystifying the Quantum Threat: Infrastructure, Institutions and Intelligence Advantage", *Security Studies*, early view, doi: 10.1080/09636412.2020.1722853.

[26] Bryan Clark, "Undersea Cables and the Future of Submarine Competition", *Bulletin of the Atomic Scientists*, vol. 72, no. 4 (2016), p. 235.

[27] Including: Maritime (semi) Autonomous Systems for Mine Countermeasures (MAS MCM), Harbour and Maritime Surveillance and Protection (HAMSPRO), Upgrade of Maritime Surveillance, Deployable Modular Underwater Intervention Capability Package (DIVEPACK) and the Maritime Unmanned Anti-Submarine System (MUSAS).

[28] Carl Benedikt Frey *et al.*, "Technology at Work: The Future of Innovation and Employment", Joint Oxford Martin School/University of Oxford and Citi Bank report, February 2015, p. 13.

[29] See, for example, the Technology for High Speed Mixed Signal Circuits (THIMS) project supported by the EDA: https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/01/19/new-chip-developed-under-eda-project-gets-award.

[30] European Defence Agency, "EDA Studies Points towards Big Data Potential for Defence", December 18, 2017, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/12/18/eda-studies-points-towards-big-data-potential-for-defence.

[31] European Commission, "Pilot Projects and Preparatory Actions – Emerging Game-changers", March 19, 2019, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/padr-fddt-emerging-03-2019;freeTextSearchKeyword=;typeCodes=1;statusCodes=31094501,31094502,31094503;programCode=PPPA;programDivisionCode=null;focusAreaCode=null;crossCuttingPriorityCode=null;callCode=PADR-FDDT-2019;sortQuery=openingDate;orderBy=asc;onlyTenders=false;topicListKey=callTopicSearchTableState.

[32] Felix Richter, "Amazon Leads $100 Billion Cloud Market", *Statista*, February 11, 2020, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

[33] European Commission, "Communication on a European Strategy for Data", *COM(2020) 66 final*, Brussels, February 19, 2020, p. 8.

[34] See the appendix of the "Communication on a European Strategy for Data", p. 26.

Published by the EU Institute for Security Studies
and printed in Luxembourg by the Publications Office of the European Union.
Cover image credit: DICOD/CREATION/REDACTION

Publications Office
of the European Union

PRINT
ISBN 978-92-9198-870-9 CATALOGUE NUMBER QN-AK-20-004-EN-C ISSN 2599-8943 DOI 10.2815/12052
ONLINE
ISBN 978-92-9198-871-6 CATALOGUE NUMBER QN-AK-20-004-EN-N ISSN 2315-1110 DOI 10.2815/766401