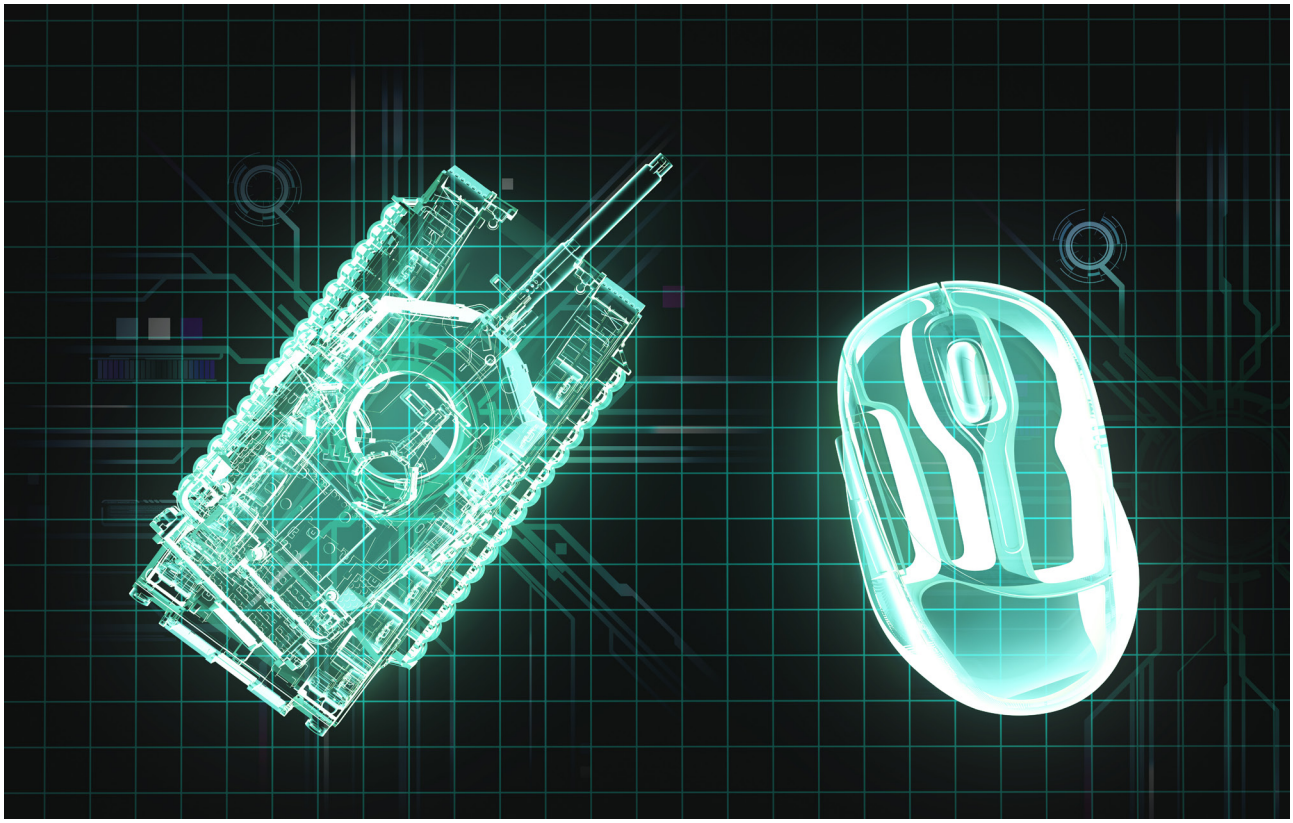
Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age

Dr Simona R. Soare

August 2023



IISS
The International Institute
for Strategic Studies

Contents

Cover

Digital illustration of tank and computer mouse (Maciej Frolow/Getty Images).

Executive Summary

NATO and the EU have embarked on a process of digital transformation of defence. In 2022 and 2023, NATO adopted its first-ever Digital Transformation vision and a Digital Transformation Implementation Strategy, while the EU endorsed a Strategic Implementation Plan for the Digitalisation of EU Forces, integrated cyber effects in EU military operations and prioritised digital capabilities under the fourth pillar (investment) of its Strategic Compass document. Subject to sectoral strategies, different elements of digital transformation – including data, cloud and the Internet of Things – are increasingly connected, contributing to the digitalisation of defence as an enabler of multi-domain operations and defence innovation through the application of emerging and disruptive technologies.

Digital transformation entails a profound socio-technological and organisational change – beyond digitisation, which is merely translating analogue data into ones and zeros. This paper outlines the principal tenets of digital-transformation initiatives in NATO and the EU, provides a brief overview of the level of digitalisation of defence in selected European countries, and analyses the key challenges of the digital transformation of defence capabilities in Europe.

The digital-transformation initiatives in NATO and the EU are having a positive impact as European governments pursue a path of incremental optimisation of digital capabilities up to the 2030s. European security will benefit from the exchange of best practices around digital transformation, the establishment of common technical standards and data-sharing policies, and the coordination of digital capability requirements and goals in defence planning.

The scope of digital transformation is ambitious in both NATO and the EU. It includes technological, organisational-procedural and people pillars of transformation and prioritises data, cloud and an updated approach to cyber security. However, implementation is hampered by the long time frames for digital transformation (into the 2030s), the lack of progress in crucial procedural components (not least procurement and budgetary alignment), challenges around data sovereignty and accessibility, and persistent underinvestment in digital capabilities for defence across Europe. Unless major change occurs across all these domains in the short term, both NATO and the EU are unlikely to achieve their digital-transformation milestones by 2030.

1. Introduction: Making Sense of Digital Transformation

A well-functioning and secure digital enterprise and force will be key enablers of the planned technological transformation of European armed forces. Both are prerequisites to embracing multi-domain integration and achieving decision superiority in today's strategic environment. Although not especially glamorous, the digitalisation of defence is an essential precursor to many capabilities that receive a lot of attention, including target-identification and acquisition algorithms; autonomy-in-motion (notably, autonomous systems); quantum cryptography and sensing; software-defined defence; and multi-domain operations where complex and self-modifying networks of sensors and shooters enable rapid decisions and action across traditional domains of warfare.[1]

This paper assesses the state of play in the level of digitalisation of defence across Europe. Sections Two and Three analyse the principal tenets of the digital-transformation agenda in NATO and the digitalisation of defence in the EU. Section Four frames the scope of the challenge entailed by digital transformation and outlines the risks associated with further delays in progressing this agenda to transform European defence.

Digital transformation is not a clear-cut concept. Digitalisation encompasses more than digitisation (which is often referred to in transformation strategies). Digitisation is the transformation of analogue data into ones and zeros, the use of information and communications technology to disseminate and analyse data, the electrification of military infrastructure with Wi-Fi networking and the use of internet portals in smart-recruitment and -procurement processes. Digitalisation, on the other hand, is not about using email and computers to crunch data and generate PowerPoint presentations. Nor, at the other end of the spectrum, is digitalisation about deploying artificial intelligence (AI) alone. Instead, it is a precursor to – and enabler of – the adoption of more sophisticated technologies, including AI, quantum and others.

Digital transformation, as designated by NATO policy, or digitalisation of defence, as it is known in EU circles, is the process of building and upgrading the digital enterprise and force – and keeping it secure. Digital transformation is about high-resolution, synchronised digital dashboards and databases comprising secure, accurate, real-time, multi-source and readily actionable data that can be accessed and used simultaneously by different security-protocol levels regardless of their geographical position. It is about data-centric networks of sensors, effectors and decision-makers (regardless of their military domain) that enable faster decision-making and action. It is equally about enhanced situational awareness including of the reliability of (and risks associated with) critical supply chains for security and defence. By leveraging new skills, processes and technologies, digital transformation entails the transformation of the defence enterprise and force from payroll to payload.

Therefore, the digitalisation of defence is only partially about the use of digital technologies. Essentially, digital transformation is a transformation process that entails profound changes in organisational policies, culture and skillsets to ensure that routine processes go from being analogue and manual to automatic and autonomous – via virtualisation, Application Programming Interfaces (APIs), cloud- and edge-computing infrastructure, next-generation communications, aligned cyber-security and -defence policies and, critically, a mature defence-data-management system. It is about the discoverability, labelling, securing, availability and exploitation of big data as a strategic asset in security and defence. It is about achieving greater situational awareness in real-time across the enterprise and the force to support decision-making and effectiveness and efficiency in subsequent military action. In short, the digitalisation of defence is a process of scalable and exponential optimisation of defence efficiency and effectiveness – both in the enterprise and the force – and an essential precursor of software-defined defence and emerging-technologies adoption.

National initiatives to prioritise digital transformation of defence and ongoing efforts within NATO and the EU are a step in the right direction. However,

as currently conceived and planned – in national capitals and the two organisations – European digitalisation of defence is insufficiently understood, too incremental and lacking sufficient scope to transform European defence at the speed of relevance. Despite the policy narrative around recognising 'the urgency of a digitally-transformed Alliance', NATO's development of the digital-transformation agenda has been years in the making.[2] Furthermore, its implementation process linked to capability development is, in fact, a decades-long process in which 2030 (for NATO, even later for individual allies) is only the first milestone of basic capability levels.[3] Both NATO and the EU seem resigned to what is regarded as a fast-follower approach to digitalisation, where neither states, nor the EU or NATO are writing the rules of the road in digital transformation of defence but are responding to much larger structural transformations around the digital revolution in industry.[4]

Europe's efforts to transform its defence and to become a competitive and credible defence actor are not making enough progress. Its poor track record on digitalisation of defence over the past few decades suggests that its defence leadership has not fully embraced the challenge. Europe has persisted with an approach to digital transformation that is characterised by incrementalism of choice and selective implementation. It has done so even in the face of strategic threats to European defence, not least that manifested in Russia's war of aggression against Ukraine, demonstrating a degree of strategic paralysis in Europe. The following sections lay out these challenges in more detail.

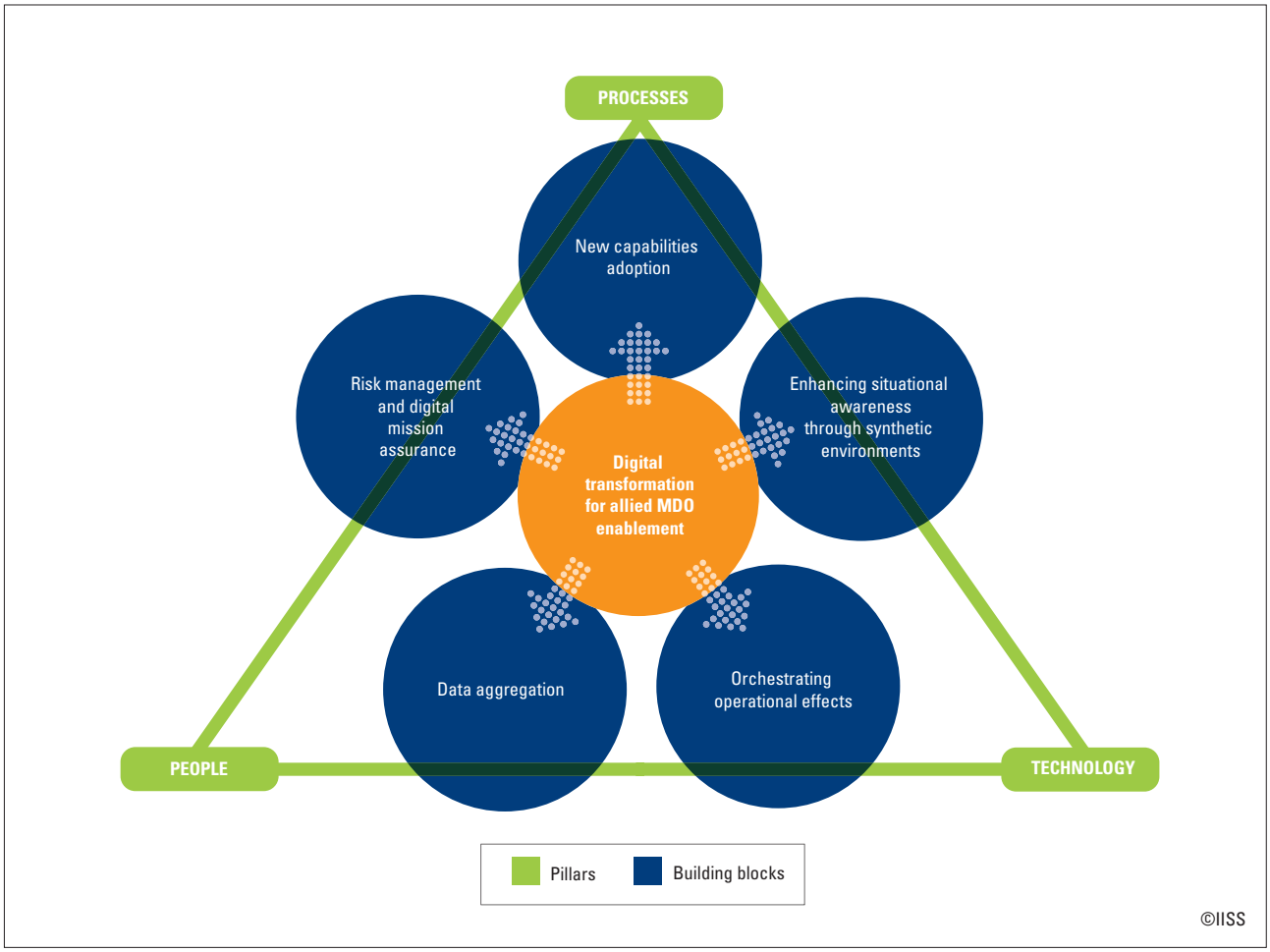
2. NATO's Digital Transformation

Digitalisation of defence is beginning to gain traction within NATO. In October 2022, member-state leaders endorsed the Alliance's vision for digital transformation and adopted a NATO Data Exploitation Framework Policy (DEFP).[5] Moreover, in July 2023, members adopted the Digital Transformation Implementation Strategy, linking digital-transformation milestones to capability-development goals and interoperability requirements.[6]

NATO's vision and implementation strategy conceive of digital transformation as a foundational enabler and driver of 'unrelenting convergence' towards multi-domain operations.[7] According to the Alliance's Digital Transformation Champion and Special Advisor Didier Polomé, by 2030, 'the NATO digital transformation will enable the Alliance to conduct Multi-Domain Operations (MDO), ensure interoperability across all domains, enhance situational awareness and facilitate political consultation and data-driven decision-making'.[8]

The strategy is grounded in operational requirements derived from various NATO documents, including its 2019 Military Strategy, its Warfighting Capstone Concept, its emerging concept for multi-domain operations, its AI Strategy and the DEFP. Individually and collectively, these documents indicate the direction of travel towards allied multi-domain operations by 2030. In addition to the war-fighting aspects, NATO's digital transformation

Figure 1: **Pillars and building blocks of NATO's Digital Transformation to enable multi-domain operations (MDO) in 2030**



is meant to be organically linked to NATO's Defence Planning Process; its capability-development goals for digital, with standardisation processes; research and development; its procurement structures; and its deep-tech structures, such as the Defence Innovation Accelerator for the North Atlantic (DIANA).

Digital transformation in NATO rests on five building blocks and three pillars, as illustrated in Figure 1. Its key technology enablers are: cloud; a modular-architecture, open-system-based digital backbone; a federate synthetic environment; and a smart data fabric, which enables all platforms and systems to process data from all sources and share them with all users. It also requires a 'zero trust' approach to cyber security.[9] Perhaps even more challenging than the technology aspects is the development of an underpinning 'culture shift which encourages and rewards innovation, experimentation, data-sharing and calculated and informed risk-taking'.[10] Finally, digitalisation of defence requires a digitally literate (and progressively a digitally native) workforce in the Alliance and member-state capitals. NATO's internal assessment is that by 2030 the Alliance will need at least 10% of its workforce to be digitally literate – a fifth-fold increase from current levels – to sustain the digital transformation.[11]

The scale of NATO's digital-transformation strategy is ambitious. However, its implementation timeline and the division of competencies within the organisation are cause for concern. Firstly, the division of labour for driving digital transformation is complex and often misunderstood within the organisation and by industry. Allied Command Transformation and Allied Command Operations are expected to drive the operational aspects of digital transformation and set requirements for digital-transformation-informed capability goals. The NATO Communications and Information Agency, the NATO Support and Procurement Agency and the Alliance's chief information officer (CIO) play a supporting role. NATO International Staff – mainly the CIO and the Emerging Security Challenges Division, as well as the Consultation, Command and Control Board – are tasked with driving the political and policy aspects of digital transformation. Although this division of labour is not unusual for large organisational bureaucracies such as NATO, inter-agency cooperation has sometimes faltered within the organisation, posing challenges on several fronts.[12]

NATO regards digital transformation as a continuous process of modernisation and optimisation. 2030 is considered the first major milestone for capability and capacity delivered in digital terms. However, according to industry and government officials, concept development around digital capabilities in European countries takes approximately two to three years on average. Procurement is a slow process that can double or triple the initial concept-development phase. Furthermore, delivery timelines for digital capabilities can take an additional three to four years, or longer, depending on the client. At present, developing and implementing a digital-enterprise roadmap and subsequent specific digitalisation projects in European defence takes at least a decade.[13]

Without urgent and radical changes in national and collective procurement processes for digital capabilities, significant alignment in budgetary outlooks and defence planning, and an exponential increase in digital skills across the NATO defence enterprise (as well as across national defence enterprises), achieving the desired level of digitalisation within the Alliance by 2030 seems unfeasible. While optimisation in digitalisation might be possible during this period, within NATO, the European pillar in particular will struggle to meet earmarked digital-transformation capability goals by 2030.

3. The EU's Road Towards Digitalisation of Defence

The EU has come a long way in its thinking about its strategic and technological sovereignty, particularly regarding security and defence. The EU Military Committee (EUMC) has been developing an agenda for the digitalisation of defence since 2019.[14] The European Commission (EC), EUMC and the European Defence Agency (EDA) are actively working on different aspects of the digitalisation of European defence, either through the European Defence Fund (EDF) or other EU-level instruments. The EDF – which sustains key digital-transformation capability-development projects – along with the EC's Directorate-General for Defence Industry and Space, the EDA and the EU Military Staff, are important actors helping to develop a better understanding of the technological landscape in Europe. The work undertaken by these actors also reduces dependencies and vulnerabilities that arise from identified gaps and highlights opportunities for civil-military and cross-border coordination.[15]

In 2019, a food-for-thought paper on 'Digitalization and Artificial Intelligence in Defence', jointly published by Finland, Estonia, France, Germany and the Netherlands, emphasised the importance of digitalisation of defence across Europe as a precursor to modernisation through the adoption of AI.[16] The EUMC discussed the same topic in internally circulated documents, including plans to launch a process of defence modernisation through the digitalisation of European armed forces. This process culminated in the endorsement of the Strategic Implementation Plan for the Digitalisation of EU Forces in 2021, which provided a gap analysis and set a level of ambition and specific targets and milestones for the digitalisation and interoperability of European armed forces.

Despite these positive steps, at this time the EU lacked a collective strategy for joint operations in security and defence. It did not have a common understanding of the role of new technologies in enhancing European defence. There were also significant gaps in the use of digital capabilities and cyber tools for defence during joint EU operations. More importantly, the EU lacked (and still does, to some degree) a clear understanding of the level of digitalisation of defence among European armed forces. No such data or assessment was immediately available even as members regularly shared information about investment, readiness levels, capability goals and shortfalls.

Subsequent concepts on strategic EU command-and-control capabilities, mission readiness, integration of cyber effects in defence, and data-sharing have partially addressed these issues. However, much work remains to be done – in cryptography, cloud, and next-generation communications, among other areas. The EU's Strategic Compass further emphasised modernisation and investment in digital and new technologies as one of the four priority pillars for action in European defence. However, investment goals remained elusive[17] and ongoing EDF capability-development projects follow traditional paths with delivery timelines into the next decade. While funds for the digital transformation of defence are larger within the EU than in NATO, implementation is infinitely slower. Prioritisation of the EU Rapid Deployment Capacity (RDC) within the EU suggests that efforts towards enhanced digitalisation of defence will concentrate on the RDC's components, underlining the limited exploitation of the digitalisation of defence.[18]

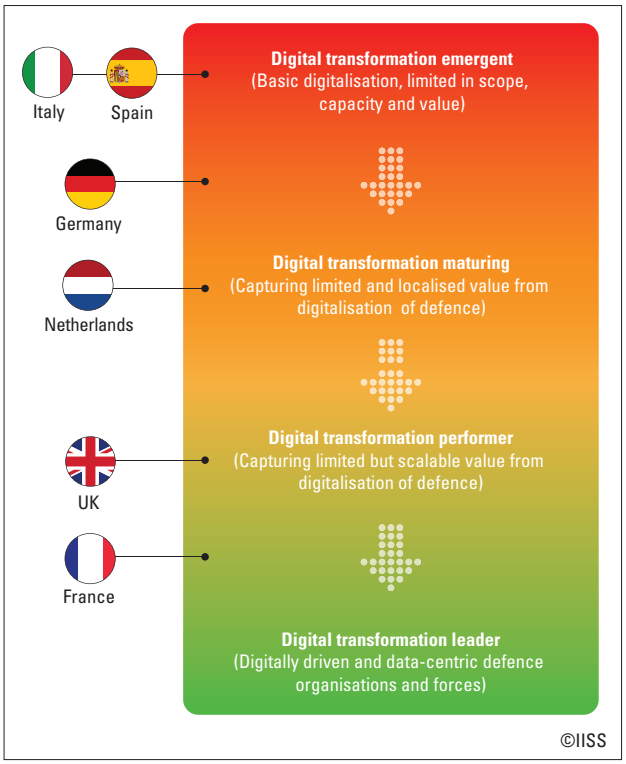
4. Digital Transformation: The Daunting Scope of the Challenge

Digital Diversity in Defence

The digitalisation of defence is not a new phenomenon in European defence. The use of information and communications technology (ICT) across European armed forces – and the use of secure ICT equipment and licensed software outside hardened defence locations – has increased exponentially over the past three years, particularly under the impact of COVID-19 restrictions. The same has been the case for NATO and the EU. Most European armed forces use at least some digital technologies and defence enterprise resource planning (EPR) systems. They also run partially digitalised defence enterprises and forces. Figure 2 highlights generic comparative levels of digitalisation of defence across Europe.

A small number of allies are seeking greater proficiency in advanced operational and tactical digitalised combat networks and command, control, communications, computers, intelligence, surveillance, target acquisition, and reconnaissance (C4ISTAR). For example, the UK is building a singular and secure 'Digital Backbone', a 'Digital Foundry' and a 'Digital Function' for its defence enterprise and force.[19] It seeks to integrate and replace 'over 2,000 [legacy] systems and applications for 200,000 users, ranging from administrative and back-office IT to military platforms such as ships and satellites', many of which are obsolescent or obsolete.[20] The 2023 Defence Command Paper, published by the UK's Ministry of Defence, pledged that digital transformation would accelerate.[21] Similarly, France's project ARTEMIS.IA (Architecture for Processing and Massive Exploitation of Multi-source Information and Artificial Intelligence), now in its third and final phase of development and roll-out, is creating not just a 'digital backbone' for its armed forces but also the technological and infrastructure foundations of digital autonomy in defence and sovereign AI.[22] Estonia, Finland, Italy, the Netherlands, Norway, Spain and Sweden – to name a few – operate defence enterprises and military units with variable levels of digitalisation. Some already use data-, software- and even infrastructure-as-a-service agreements with various industry actors.

Figure 2: **Levels of digitalisation of defence in selected European states**



Still, European countries must overcome significant challenges if they are to complete the digitalisation of their defence enterprises. Most lack or are still maturing integrated digital defence-data-management systems. They use physical hardened on-site and on-board data-storage infrastructure. And a significant proportion of European states face difficulties in maintaining and regularly upgrading their digital systems. Some have even gone a decade or longer without performing security-critical updates and upgrades to their key information systems.[23] The use of defence cloud across Europe remains very limited, with three countries and a multinational organisation (France, Germany, the UK and NATO) using it at service level or in federated networks. In addition, the EU's European Defence Fund provides financial support for projects focused

on defence cloud storage and collaborative defence cloud networking solutions. Yet with less than 1% of cloud-services providers across Europe being European companies, the issue of sovereignty is bound to arise.[24] Indeed, data sovereignty is an underpinning principle of digital transformation in both NATO and the EU. While technical solutions exist to protect data sovereignty and to secure the data itself, cross-border and cross-domain data-sharing will remain a challenge in the medium term for both organisations.

For example, many European armed forces still widely log and report personnel and equipment readiness manually. Maintenance and logistics gaps are a regular occurrence as reporting on the maintenance work on deployed equipment is backlogged. Most recently, EU and NATO members faced significant challenges in rapidly reporting ammunition stocks for the EU-level initiative in common procurement that aimed to aid efforts to replenish ammunition stocks following their support of Ukraine's war effort.[25]

Digital Underinvestment

While European states are incrementally increasing their investment in digital capabilities, data compiled by the International Institute for Strategic Studies (IISS) shows that the estimated level of European national spending on digital capabilities – including digital enterprise and cyber security – remains low in terms of dedicated percentage of national defence budgets. In Table 1, estimated annual defence expenditure on digital capabilities among selected European countries varies between 0.4% and 8.3% of annual national defence spending. The UK spends the most on digital capabilities, investing an estimated USD5.3 billion in 2023, followed closely by France, which will spend USD2.8bn–3.2bn on digital capabilities in 2023.[26] Spain is the lowest spender on digital capabilities, investing approximately 0.4% of its annual defence budget, behind Italy and Germany. By comparison, the US will spend an estimated USD55.2bn on digital capabilities (enterprise IT, digital capabilities and infrastructures; and cyber) in FY2023, amounting to 6.8% of its annual defence spending.

Cost estimates are challenging, however. As European states do not report their expenses on IT, software, and digital services and capabilities as distinct budget lines, it is difficult to accurately assess the full extent of their expenses across investment, maintenance and decommissioning cost categories. For example, the UK 2023 estimated defence budget pledged approximately USD5.3bn for digital transformation, while in 2019 it was estimated that it would cost USD14.1bn alone to replace six critical digital systems in defence over the following decade.[27] While it can be unclear if reported annual budgets include maintenance and decommissioning costs alongside investment, the French, Italian and Spanish budgets separate investment from maintenance of digital capabilities. Efforts to accurately assess these expenses are further complicated by a lack of transparency and detail in reporting on European national defence budgets.

Nevertheless, understanding national defence expenditure for digital transformation is a prerequisite

Table 1: **Estimated annual expenditure of individual allies in NATO and the EU on digital capabilities for defence (2022–23)**

Country	Nominal defence budget (billions, national currency)	Nominal defence budget (billions, USD)	Estimated annual spending on digital capabilities (billions, national currency)	Estimated annual spending on digital capabilities (billions, USD)	Estimated digital capabilities investment as % of defence budget *
France	43.9	46.7	2.6–3.0	2.8–3.2	6.0–6.8
United Kingdom	53.1	64.5	4.4	5.3	8.3
Netherlands	15.8	16.8	0.6–1.0	0.6–1.1	3.6–6.0
Germany	50.1**	53.2	1.0–1.3	1.1–1.4	2.0–2.6
Italy	26.0	27.6	0.2–0.5	0.2–0.5	0.9–1.8
Spain	12.8	13.6	0.0557	0.0592	0.4
United States	816.7	N/A	55.2	N/A	6.8

Note: all figures have been rounded to one decimal place, with the exception of Spain's estimated annual spending on digital capabilities.
* Percentages were calculated using unrounded, national-currency values for nominal defence budgets and estimated annual spending on digital capabilities.
** Core defence budget only, does not include funding reserved for digital capabilities under the off-budget Defence Investment Fund (*Sondervermögen*)
Source: Compiled by author from multiple official sources (national, NATO and EU), 2023

to understanding governments' progress in this area. The budgetary structure of digital-transformation expenditure is significantly different from that of traditional procurement. In digital capabilities, procurement and maintenance costs are relatively balanced and similar over time; for traditional platforms, the initial procurement represents a small share of the lifecycle costs.

There is increasing awareness that military organisations across Europe lag behind other industries – certainly the big tech industry – in terms of the effective exploitation of data as a strategic, value-creating asset. Industry representatives argue that digital transformation is a time-intensive process requiring on average three to four years, depending on the specific defence client.[28] However, slow and antiquated procurement procedures and inflexible budgeting procedures often result in defence-digitalisation projects that last decades. For example, individual projects within Germany's, Italy's and Spain's defence-digitalisation initiatives have timelines ranging to 2030 (and most stretch out to 2035), while Norway's project is expected to take at least a decade to complete.[29] By comparison, digital transformation in industrial sectors takes on average under two years.[30]

Defence establishments are increasingly aware of the need to accelerate the pace of digital transformation, not least due to the experience of the war in Ukraine, where the transition from idea to practical battlefield application can sometimes be measured in weeks. Indeed, some of the technology-driven solutions actioned in Ukraine have a shelf life of only a few weeks before countermeasures or adaptation by the enemy necessitates the next evolution to maintain the edge. German Chief of Defence General Carsten Breuer argued in July 2023 that armament and procurement processes were still not fit for purpose when it came to managing the pace of innovation and the potentially disruptive effect of some technologies.[31] The UK's Defence Command Paper noted, with regards to acquisition reform, the UK's 'ambition is to reduce radically the average time from the identification of a military need to contract placement, and from contract placement to delivery to the front-line'.[32] The paper then commits to ensuring that this process takes a maximum of three years for digital programmes – perhaps not quite as ambitious as the general thrust of the paper would suggest. In NATO and EU member-state forces, digital projects that move from conception to implementation within a few months are still the exception rather than the norm.

Defence Digital Fragmentation and Siloed Data

The heterogeneity of European armed forces poses a significant challenge to digital transformation. While European allies operate thousands of defence digital systems and infrastructures, these were developed as a collection of self-contained, individual systems and function on the principle of localised exploitation of their own data siloes. This has been the case for the past three decades at enterprise, service and sub-service levels. Data policies within NATO and European armed forces are, by default, based on a need-to-know sharing model rather than a data-centric one, where data-sharing is the norm across the organisation.

Individual and unsynchronised data architectures are a major obstacle to data-sharing both within and across domains. Different military platforms operating in the same domain and in the same battle networks often use different types of data, without an underlying common data and digital architecture that enables data-sharing by default.[33] Within NATO there are already ongoing initiatives, such as the Data Exploitation Framework Policy (DEFP) and the Data Exploitation Programme (part of the Warfare Development Agenda), that attempt to increase interconnectivity among the huge variety and diversity of data environments across the Alliance. These efforts contribute to the digital-transformation agenda but do not address the need for an integrated and singular secure data environment at the enterprise level and for operational purposes among allies and NATO commands. Prioritising data- and meta-data standardisation – as well as default data-sharing rules of the road – is essential for NATO's and the EU's digital transformation of defence.

Successive waves of digitalisation have improved data-sharing and coherence at service level and – in an international context – in-domain services (e.g., navy-to-navy data-sharing, air force-to-air force data-sharing, and so on). There is currently limited data

exchange across services at the national level and within multinational organisations, such as NATO and the EU. At present, ensuring digital and data interoperability among allies and NATO or the EU is a security- and resource-intensive and technologically patchy exercise, often resulting in sub-optimal results on and off the battlefield. This situation presents significant challenges for enhanced situational awareness, combined and joint operations (and, in the future, multi-domain operations) and efficient and affordable defence management.

Smart logistics and preventive maintenance are often considered low-hanging fruit for automation as part of the digital transformation in defence. French initiatives in preventive maintenance for its *Rafale* fighter-jet fleet are good examples of ongoing digitalisation and automation in logistics and maintenance. However, more broadly, these types of initiatives are often pockets of automation at service level and rarely scale nationally, let alone internationally, even for countries using the same platform, equipment, system or subsystem. Industrial and security-related challenges persist as significant obstacles impeding the rapid rollout of automation in logistics.

Several European countries are already rolling out digital-transformation initiatives at the national level. While publicly officials emphasise the high quality of NATO allies' digital capabilities, privately they share a concern over a widening digital-capabilities gap within the Alliance and between the two shores of the Atlantic.[34] Left uncoordinated at the multinational level, the diverse range of national defence-digitalisation initiatives risk enhancing the huge technological and digital complexity of European armed forces and further reducing interoperability. Therefore, a significant challenge for the digital transformations in NATO and the EU will be aligning national initiatives and ensuring data compatibility – and digital interoperability – by default among member states and within their own organisational enterprises.

Inherent Risks of Delayed Digitalisation of Defence

In 2018 and 2019, the EU Military Staff performed a classified survey of the level of digitalisation of defence across European armed forces. While the results remain closed to the public, the officials privately assessed the level of digitalisation as not convincing.[35] Moreover, a 2021 audit report of NATO's Allied Command Operations (ACO) confirmed the poor state of affairs:

> Inadequate information management, in combination with obsolete IT infrastructure and unsatisfactory IT support, and missing links between different information systems present a critical issue for ACO. The critical operational obsolescence of the legacy system and the growing capability gap affects system support, security, performance, reliability, and through-life costs, and limits ACO's ability to fully protect and exploit data.[36]

The scope of the risks associated with these levels of digitalisation across defence in Europe cannot be understated. The ACO audit report also concluded that repeated delays in the modernisation of critical digital infrastructure and systems have exposed the alliance to 'an unacceptable level of operational risk'.[37] The prevalent view among NATO military and policy officials is that the Alliance's legacy digitalised enterprise and communication and information systems are increasingly a vulnerability rather than an operational strength.[38] The capability gaps and obsolescent legacy systems in command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) – particularly in C3 – among allies and at NATO and EU levels are one such vulnerability. Other public audit bodies in France, Germany, Italy and the UK have issued similar warnings regarding national defence digital capabilities and infrastructure. In addition, in 2017 the US Government Accountability Office criticised the Department of Defense for significant risks incurred as a result of a failure to update and upgrade critical information and digital systems, including in the nuclear domain.

Conclusion

Defence innovation, artificial intelligence and other emergent technologies preoccupy the minds of European defence ministers. However, digital transformation and the secure exploitation of data will comprise the bedrock of European defence establishments' future military power; they will need to make significant progress in these areas before European defence can seriously consider the operational integration and battlefield deployment of advanced technologies like AI. EU and NATO processes are in motion to set a common denominator and ensure coherence and interoperability among national initiatives. To succeed, digital transformation must be technologically relevant, have geographical and organisational scalability, be human-centric (people first) and, importantly, win the race against time. Modernisation, innovation, and recapitalisation of mass – as well as enhanced defence efficiency and affordability – depend on the successful and timely digitalisation of European defence.

Notes

1 On software-defined defence, see Simona R. Soare, Pavneet Singh and Meia Nouwens, 'Software-defined Defence: Algorithms at War', IISS Research Paper, 17 February 2023, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/iiss_software-defined-defence_17022023.pdf; Nand Mulchandani and Lt-Gen. (Retd) John N.T. 'Jack' Shanahan, 'Software-defined Warfare: Architecting the DOD's Transition to the Digital Age', Center for Strategic and International Studies, 6 September 2022, https://www.csis.org/analysis/software-defined-warfare-architecting-dods-transition-digital-age; and Jason Weiss and Dan Patt, 'Software Defines Tactics: Structuring Military Software Acquisitions for Adaptability and Advantage in a Competitive Era', Hudson Institute, 14 December 2022, https://www.hudson.org/national-security-defense/software-defines-tactics-structuring-military-software-acquisitions. The traditional domains of warfare are land, air and maritime; the newer domains are cyber and space. Some consider the information domain to be a domain in and of itself. However, as crucial as it is to international security, it is yet to be formally recognised as a domain of warfare by international actors.

2 NATO, 'Vilnius Summit Communiqué', 11 July 2023, paragraph 62, https://www.nato.int/cps/en/natohq/official_texts_217320.htm.

3 Author's interviews with industry, EU and NATO representatives, 2023.

4 NATO, 'NATO Digital Transformation', NATO ACT Innovation Podcast, episode 9, 23 November 2022, https://www.act.nato.int/newsroom/multimedia/podcasts/.

5 NATO, 'NATO Allies Take Further Steps Towards Responsible Use of AI, Data, Autonomy and Digital Transformation', 13 October 2023, https://www.nato.int/cps/en/natohq/news_208342.htm.

6 NATO, 'Vilnius Summit Communiqué', paragraph 62.

7 Manfred Boudreaux-Dehmer, 'Innovation and the Digital Transformation', *NITECH: NATO Innovation and Technology*, vol. 9, July 2023, p. 17, https://issuu.com/globalmediapartners/docs/nitech9_-_full_pdf_final?fr=xPf81NTU.

8 Brig.-Gen. Didier Polomé, 'Alliance Digital Transformation for Multi-Domain Operations', *NITECH: NATO Innovation and Technology*, vol. 9, July 2023, p. 39, https://issuu.com/globalmediapartners/docs/nitech9_-_full_pdf_final?fr=xPf81NTU.

9 Scott Rose et al., 'Zero Trust Architecture', National Institute of Standards and Technology, US Department of Commerce, NIST Special Publication 800-207, August 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

10 Polomé, 'Alliance Digital Transformation for Multi-domain Ooperations', p. 40.

11 NATO, 'NATO Digital Transformation', NATO ACT Innovation Podcast.

12 Simona R. Soare, 'Algorithmic Power, NATO and Artificial Intelligence', IISS Military Balance Blog, 19 November 2021, https://www.iiss.org/en/online-analysis/military-balance/2021/11/algorithmic-power-nato-and-artificial-intelligence/.

13 Author's interviews with industry representatives, 2023.

14 Author's interviews with EU officials, 2021–23.

15 See, for example, Simona R. Soare, 'Algorithmic Power? The Role of Artificial Intelligence in European Strategic Autonomy', in Fabio Cristiano et al. (eds.), *Artificial Intelligence and International Conflict in Cyberspace* (Abingdon: Routledge, 2023), pp. 77–108, https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003284093/artificial-intelligence-international-conflict-cyberspace-dennis-broeders-fabio-cristiano-françois-delerue-frédérick-douzet-aude-géry?refId=cdode83a-e929-4627-a0ee-71bab71881f6&context=ubx. Also see Raluca Csernatoni, 'The EU's Defense Ambitions: Understanding the Emergence of a European Defense Technological and Industrial Complex', Carnegie Europe, 6 December 2021, https://carnegieeurope.eu/2021/12/06/eu-s-defense-ambitions-understanding-emergence-of-european-defense-technological-and-industrial-complex-pub-85884; and Daniel Fiott, 'Digitalising Defence: Protecting Europe in the Age of Quantum Computing and the Cloud', European Union Institute for Security Studies (EUISS), brief no. 4, March 2020, https://www.jstor.org/stable/pdf/resrep25017.pdf.

16 Finnish Government, 'Food for Thought Paper by Finland, Estonia, France, Germany, and the Netherlands: Digitalization and Artificial Intelligence in Defence', 17 May 2019, https://valtioneuvosto.fi/

documents/11707387/12748699/Digitalization+and+AI+in+Defence.pdf/151e10fd-c004-coca-d86b-07c35b55b9cc/Digitalization+and+AI+in+Defence.pdf.

17 'Defence Innovation and the European Union's Strategic Compass', IISS *Strategic Comments*, vol. 28, no. 10, 30 May 2022.

18 The EU RDC will comprise those national forces contributed by member states to the rotating EU Battlegroups on standby, the pre-identified force modules earmarked by member states, and the required strategic enablers. These elements will make up the RDC once it reaches full operational capability in 2025.

19 UK, Ministry of Defence, 'Digital Strategy for Defence: Delivering the Digital Backbone and Unleashing the Power of Defence's Data', April 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990114/20210421_-_MOD_Digital_Strategy_-_Update_-_Final.pdf.

20 UK, House of Commons, Committee of Public Accounts, 'The Defence Digital Strategy', 36th report of session 2022–23, 26 January 2023, p. 3, https://committees.parliament.uk/publications/33824/documents/189511/default/.

21 UK, Ministry of Defence, 'Defence's Response to a More Contested and Volatile World', CP 901, July 2023, p.36, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1171269/Defence_Command_Paper_2023_Defence_s_response_to_a_more_contested_and_volatile_world.pdf.

22 Vivienne Machi, 'France Approves Final Phase of Artemis Big-data Processing Platform', Defense News, 11 July 2022, https://www.defensenews.com/global/europe/2022/07/11/france-approves-final-phase-of-artemis-big-data-processing-platform/.

23 Author's interview with industry representative, 2023.

24 See, for example, the Microsoft, Thales and Google contracts to provide the French government with government-trusted – or sovereign – data storage and cloud solutions.

25 Author's interviews with EU officials, 2023.

26 See UK, National Audit Office, 'The Digital Strategy for Defence: A Review of Early Implementation', 19 October 2022, p. 4, https://www.nao.org.uk/wp-content/uploads/2022/10/NAO-report-The-Digital-Strategy-for-Defence-A-review-of-early-implementation.pdf; and Assemblée Nationale, 'Rapport no 292 fait au nom de la commission des finances, de l'économie générale et du contrôle budgétaire sur le projet de loi de finances pour 2023 (n° 273), par Jean-René CAZENEUVE, Rapporteur général Député' [Report no. 292 on behalf of the Committee on Finance, General Economy and Budgetary Control on the Finance Bill for 2023], 6 October 2022. See 'La consolidation des crédits affectés au commandement et à la maîtrise de l'information' [Consolidation of appropriations allocated to command and control of information], https://www.assemblee-nationale.fr/dyn/16/rapports/cion_fin/l16b0292-tiii-a14_rapport-fond#:~:text=Le%20budget%20proposé%20pour%202023,les%20programmes%20d%27équipement%20majeur.

27 UK, National Audit Office, 'The Digital Strategy for Defence: A Review of Early Implementation', p. 4.

28 Author's interviews with industry representatives, 2023.

29 *Ibid*.

30 Garima Bora, 'How Long Does It Take to Digitally Transform Your Small Business?', *Economic Times*, 28 March 2023, https://economictimes.indiatimes.com/small-biz/sme-sector/how-long-does-it-take-to-digitally-transform-your-small-business/articleshow/99025434.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

31 Unofficial transcript of the speech available at: Thomas Wiegold, 'Bundeswehr-Generalinspekteur fordert von Streitkräften: „Gewinnen wollen. Weil wir gewinnen müssen" (m. Redetext)' [Bundeswehr chief demands of armed forces: 'Desire to win. Because we must win'], 13 July 2023, https://augengeradeaus.net/2023/07/bundeswehr-generalinspekteur-fordert-von-streitkraeften-gewinnen-wollen-weil-wir-gewinnen-muessen/.

32 UK, Ministry of Defence, 'Defence's Response to a More Contested and Volatile World', p. 41.

33 Soare, Singh and Nouwens, 'Software-defined Defence: Algorithms at War', p. 7.

34 Author's interviews with NATO officials, 2021–23.

35 Author's interviews with EU officials, 2021–23.

36 NATO, 'IBAN Audit Report on the Audit of 2021 Consolidated Financial Statements of Allied Command Operations (ACO)', PO(2022)0504-AS1 (INV), 16 December 2022, https://www.nato.int/issues/iban/financial_audits/2021-ACO-en.pdf. See Section '2021 ACO Statement of Internal Control', p. 1.

37 *Ibid*.

38 Author's interviews with NATO officials, 2021–23.

Acknowledgements

The IISS thanks SAP for supporting research that informed the drafting of this research report.

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **f.** +44 (0) 20 7836 3108 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 600 | Washington DC 20037 | USA
t. +1 202 659 1490 **f.** +1 202 659 1499 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **f.** +65 6499 0059 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Europe
Pariser Platz 6A | 10117 Berlin | Germany
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GFH Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **f.** +973 1710 0155 **e.** iiss-middleeast@iiss.org