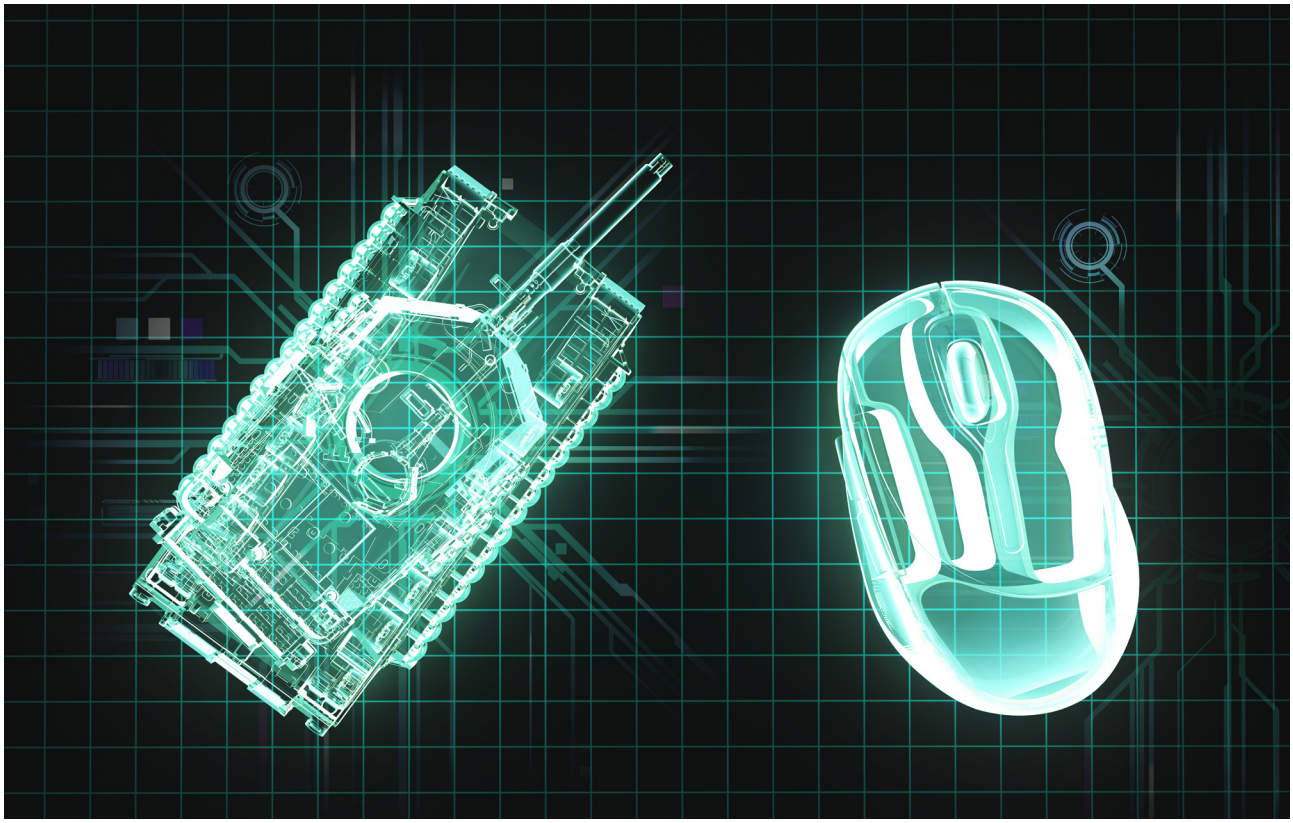
Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age

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,