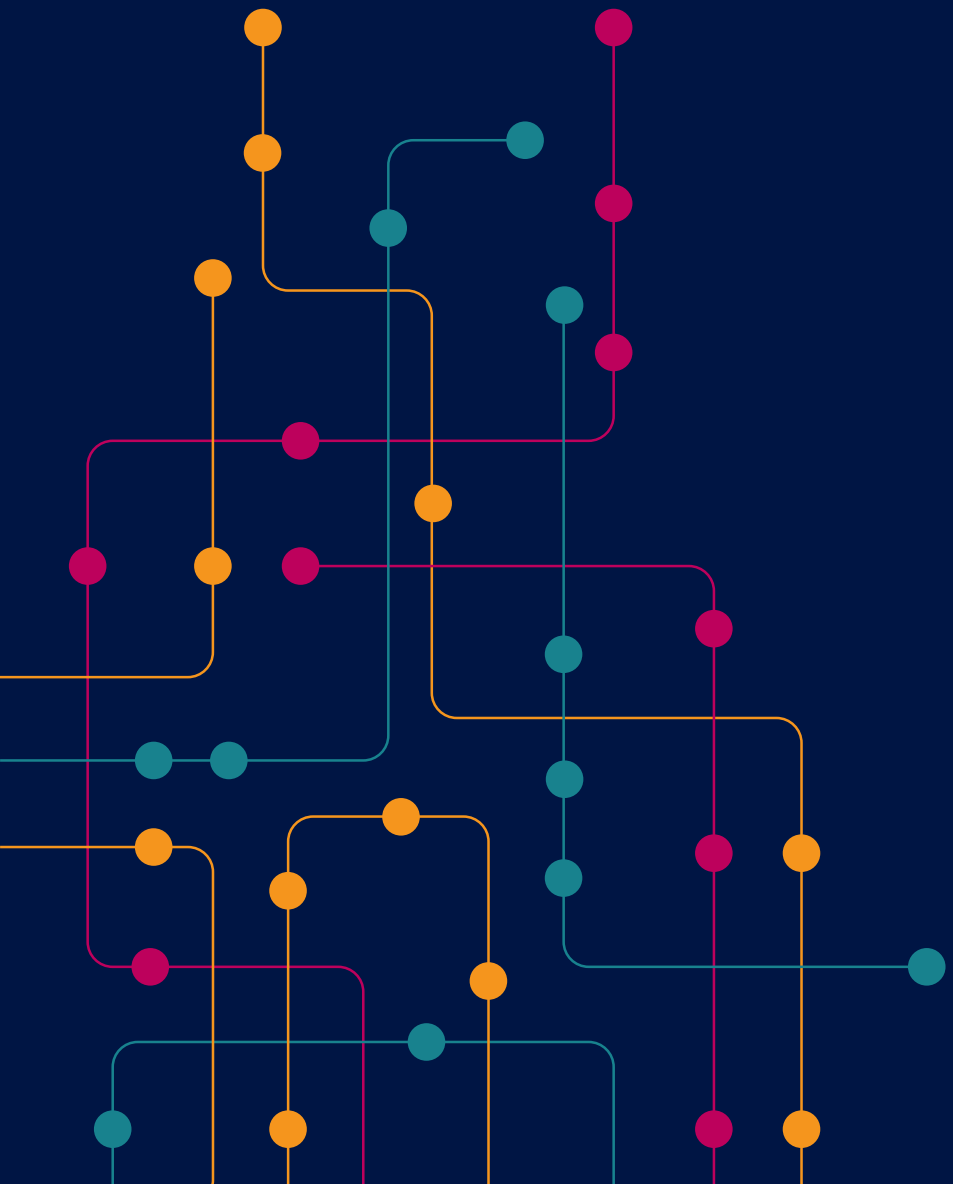
RAND EUROPE

Conceptualising digital capability

Enabling NATO digital capabilities series: Paper 1

Judith Huismans, Rebecca Lucas, Ondrej Palicka, Sarah Winder, Erik Silfversten



For more information on this publication, visit www.rand.org/t/RRA3831-1

About RAND Europe
RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit www.randeurope.org.

Research Integrity
Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

Cover: Adobe Stock

Preface

This is the first in a series of three papers exploring the evolving role of digital capabilities in the North Atlantic Treaty Organization (NATO). This paper seeks to develop a clearer conceptual understanding of digital capability, its relationship to digital transformation, and how digital capabilities are supporting the core tasks of the Alliance.

The other two papers will explore:

- Implications and enablers of effective digital capability management (April 2025).
- Opportunities and challenges of interoperability in the digital environment (May 2025).

The papers were sponsored by Microsoft as part of a broader package of work to explore how NATO and its members can progress the development of digital capabilities, how the development of such capabilities can be more effectively enabled, and how these capabilities can enhance NATO's resilience and interoperability. The full series of papers is intended to drive preparatory discussions on the importance and future of NATO's digital capabilities ahead of the June 2025 summit in The Hague.

RAND Europe had full editorial control and independence of the analyses performed and presented in this report, which has been peer-reviewed in accordance with RAND Europe's quality assurance standards. Our work is intended to inform the public good and should not be taken as a commercial endorsement of any product or service.

About RAND

RAND Europe is the European arm of RAND, an independent, not-for-profit research institute that aims to improve policy and decision making through objective research and analysis. RAND's clients include governments, militaries, inter- and non-governmental organisations, and others with a need for rigorous, independent and interdisciplinary analysis.

For further information on RAND or this study, contact:

Judith Huismans
Research Leader – Defence, Security & Justice Research Group, RAND Europe
RAND Europe
Gardens Business Centre New Babylon
Anna van Buerenplein 41
2595 DA The Hague
The Netherlands
jhuismans@randeurope.org

Summary

A lack of shared understanding of key terminology may hinder NATO–industry collaboration and prevent successful digital capability development.

Our analysis reveals a lack of universally accepted definitions of ‘digital’, ‘digital capability’ and ‘digital transformation’, particularly within defence. These terms are often used interchangeably, leading to tensions, especially between civilian or industry contexts and NATO contexts.

In NATO, the term ‘digital’ is broad, encompassing the integration of digital technologies in military operations and organisational frameworks. This includes traditional IT as well as communications and information systems (CIS) and extends to cyber defence, data standardisation, digital interoperability and emerging technologies. It comprises both enabling and effector capabilities, with applications both to military operations and to ‘back office’ functions.

NATO refers to ‘capability’ as the ability to create an effect through employment of

an integrated set of aspects categorised as doctrine, organisation, training, materiel, leadership development, personnel, facilities and interoperability. This approach emphasises NATO's view of capability as a broad, system-level concept.

Within the Alliance context, it is also important to distinguish between NATO-owned and -operated capabilities and national capabilities specific to individual countries, as well as to recognise the growing role of commercial suppliers in maintaining and deploying digital capabilities. This distinction and role present a more complex context for integration and interoperability than more traditional domains or non-digital capability areas, as the software-driven nature of many digital technologies necessitates much faster capability upgrade cycles and feedback loops from end users back to industry.

The conception of 'digital transformation' also varies with some viewing it as time- and resource-bound and others seeing it as a continuous process that complements digital capabilities. NATO's *Digital Transformation Vision* and accompanying *Digital Implementation Strategy* emphasise the latter approach, with transformation focused on ongoing and long-term efforts. Digital transformation within NATO is, therefore, an ongoing and iterative process that seeks to facilitate the development of the next generation of digital capabilities while remaining adaptable to innovation across the Alliance's people, processes, technology and data.

Our main recommendation is therefore to foster shared understanding of these terms, which is vital for effective cooperation across NATO and with industry and the science and technology community, particularly with partners new to working in defence. A common lexicon can minimise misunderstandings, align stakeholders, and foster trust, all of which is essential for standardisation and interoperability, thereby aiding NATO in achieving its digital ambitions.

Digital capability is a key enabler for NATO's core tasks, and successful digital capability development will be essential for the future success of the Alliance

The paper has also explored the role of digital capabilities in the context of NATO's core tasks. The Alliance continues to be the foremost pillar of transatlantic security and an important element of the global international order. For NATO to fulfil its core tasks, it will need to achieve the desired strategic objectives as outlined in the *Digital Transformation Implementation Strategy*. Table S.1, below, illustrates how digital capabilities may contribute to NATO's core tasks.

This is the first in a series of three papers exploring the evolving role of digital capabilities in the NATO Alliance. The second paper will cover implications and enablers of effective digital capability management and explore:

- Barriers and enablers to effective digital capability development in NATO
- Possible implications of digital capability development for defence spending across NATO
- Possible implications of underinvestment in digital capabilities

The third paper will cover the topic of interoperability in the digital environment and explore:

- Opportunities and challenges for fostering greater interoperability in the digital environment (particularly considering growing demands for digital sovereignty among NATO Allies)
- Implications of fostering digital interoperability for European strategic autonomy, the European defence industry and defence industrial cooperation within NATO.

Table S.1 Illustrative examples of ways digital capability contributes to NATO core tasks

Core task	Ways digital capabilities can enable the core task
Deterrence and defence	Digital capabilities enhance NATO's collective defence by facilitating military operations and coordination among Allies through services such as C4ISR and through: • Multi-domain operations (MDO): Technologies, such as advanced communications systems and artificial intelligence (AI), enable 'digital-ready combat forces' to conduct MDO, supporting real-time data sharing and situational awareness for synchronised military and non-military activities. • Enhanced situational awareness: Systems such as NATO's Alliance Data Sharing Ecosystem improve interoperability and operational effectiveness by providing a comprehensive view of the battlespace and facilitating real-time data sharing.
Crisis prevention and management	Digital technologies enhance resilience by enabling early detection and response to crises, ensuring continuity of operations and effective management of critical infrastructure.
Cooperative security	Digital capabilities support interoperability among Allies, allowing for effective joint military operations through secure communication systems and data-sharing platforms via: • Interoperability: Robust digital communication and information systems, along with standardisation efforts, are essential for achieving seamless collaboration across various technological levels. • Political consultation and data-driven decision making: Digital tools, such as those of the NATO Intelligence Fusion Centre or Supreme Headquarters Allied Powers Europe (SHAPE), facilitate secure sharing and analysis of intelligence, ensuring informed and timely decision making.

Source: RAND Europe analysis.

CONCEPTUALISING DIGITAL CAPABILITY

Digital capability is a key enabler for NATO's core tasks, and successful digital capability development will be essential for the future success of the alliance. However, our analysis reveals a lack of universally accepted definitions, particularly between defence and non-defence stakeholders.

CORE DEFINITIONS

Digital: The integration of digital technologies in military capability and organisational frameworks. This includes:

- Traditional IT
- Communications & information systems
- Cyber defence
- Data
- Digital interoperability
- Emerging and disruptive technologies

Capability: The ability to create an effect through an integrated set of aspects:

- Doctrine
- Organisation
- Training
- Materiel
- Leadership development
- Personnel
- Facilities
- Interoperability

Digital transformation: NATO views digital transformation as a continuous and iterative process to develop the next generation of digital capabilities, while remaining adaptable to innovation across the alliance.

HOW DOES DIGITAL CAPABILITY SUPPORT NATO'S CORE MISSION?

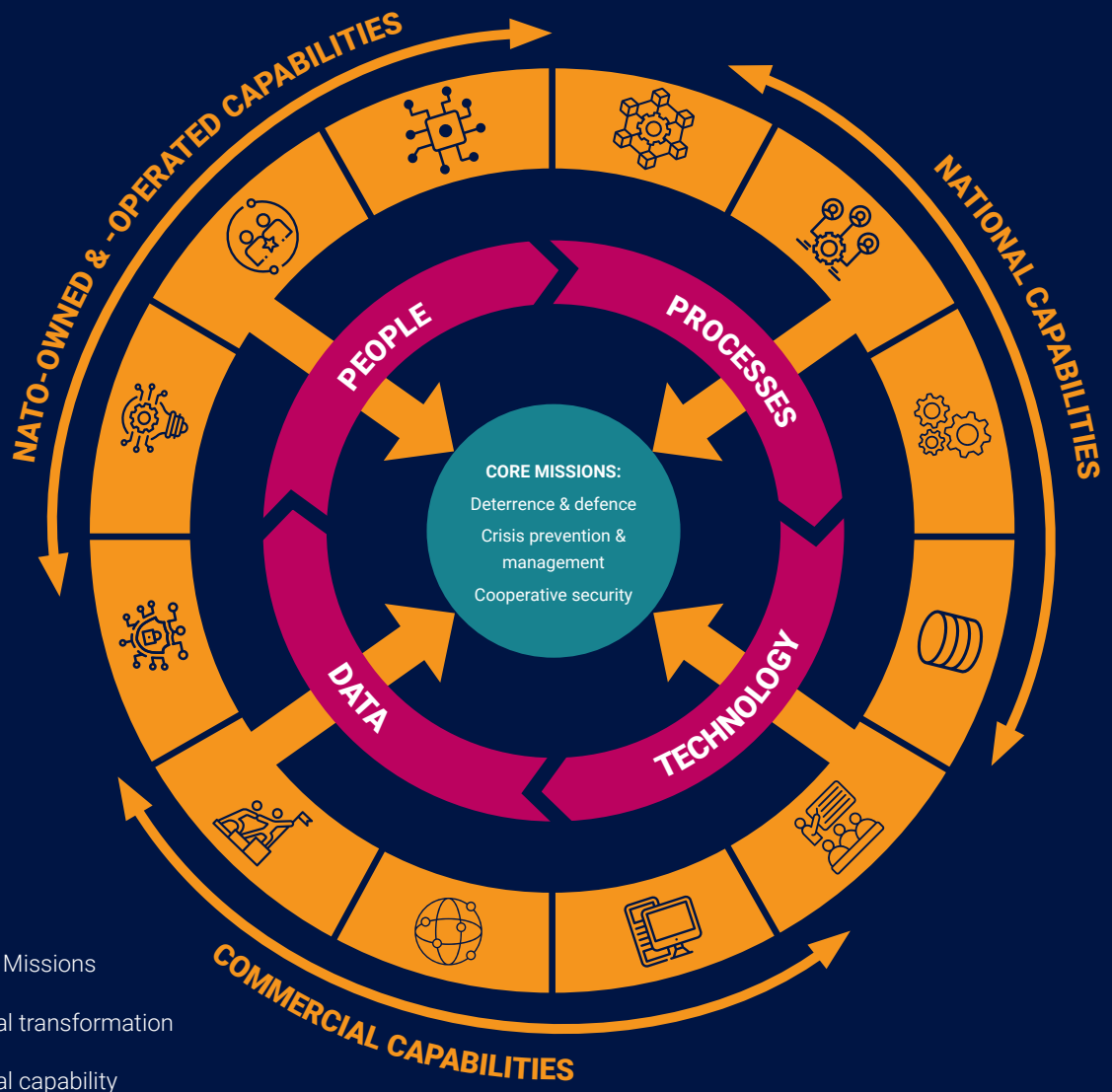


Table of contents

Chapter 1. Introduction and background

1.1. Background

When Allied leaders gather for NATO's Hague Summit, in June 2025, they will face several complex and challenging issues. Of the questions that will be put to them, few are more all-encompassing than how NATO should approach its integration and use of new technology. Development of digital capabilities that enable activities including data collection, analysis and sharing, as well as communication and coordination among Allies, has been a key line of effort (LOE) for the Alliance for several years now. Their importance has been pointed out in key documents, including NATO's *2022 Strategic Concept*, the NATO 2030 initiative and the *Digital Transformation Implementation Strategy* that NATO issued in autumn 2024.[1]

Microsoft has commissioned papers from a series of different research organisations and think tanks, including RAND Europe, to explore how NATO might best approach these issues. These are set to appear in the months leading up to the Summit.

Specifically, the questions posed to RAND included how NATO should approach digital capabilities, barriers and enablers to their acquisition, as well as challenges and opportunities around issues of interoperability and digital sovereignty.

1 NATO (2022a; 2025).

This paper, the first in a series of three from RAND, explores how digital capability can best be defined and how it can contribute to NATO's core tasks.

1.2. Research approach

This paper explores three questions:

1. What is digital capability?
2. Does digital capability differ from digital transformation and if so, how?
3. What is the role of digital capabilities in the context of NATO's key strategic priorities?

To address these questions, the research team combined three methods:

- A rapid evidence assessment to review relevant literature on existing definitions and conceptualisations of digital capability and digital transformation.
- Interviews with NATO stakeholders and experts working in the fields of digital security and cybersecurity, to explore their perspectives on digital capability in an Alliance context.
- A series of case studies to better understand not only how NATO as an organisation approaches digital capabilities, but also how selected Allies (Estonia, Finland, Poland and Sweden) do so in their own national defence ecosystems.[2] These case studies enriched the discussion by drawing out similarities and differences in national approaches to digital capability development, enabling the research team to identify examples, possible gaps and good practice.

1.3. Outline

This paper proceeds as follows:

- **Chapter 2** describes the evolving understanding of the definition of digital capability, and how it compares to and complements NATO's definition of digital transformation.
- **Chapter 3** explores how digital capabilities support NATO as an organisation, as well as enable the Alliance's strategic priorities.
- **Chapter 4** summarises the conclusions of this paper and looks ahead to the next two in the series.
- **Annex A** presents the case studies of digital capability and transformation in Estonia, Finland, Poland and Sweden. These case studies also inform the analyses in Chapters 2 and 3.

2 These countries represent a selection of NATO Allies known for their digital capabilities and others that have recently increased their investment in this space. The selection of case studies was discussed and agreed together with Microsoft.

Chapter 2. Understanding digital capability

In this chapter, we examine the evolving concept and connotations of 'digital' within the context of NATO capability development and analyse the relationship between digital capability and NATO's evolving perspective on digital transformation. Our research has two key findings:

- There are no commonly shared definitions of the terms 'digital', 'digital capability' and 'digital transformation'.
- Tensions exist in the usage of these contested terms, particularly between civilian or private-sector uses of digital technologies, on the one hand, and their distinctive applications in military or NATO contexts, on the other.

2.1. 'Digital' and its relationship with 'cyber'

'Digital' is a broad umbrella term commonly used in relation to digital technologies (e.g. electronic devices, such as computers), digital media (e.g. information, audio and video), and digital communications (e.g. emails and instant messaging).[3] Its use as a prefix can make it challenging to define and understand this word accurately.

3 Yasar (2023).

While NATO's official terminology database (*NATOTerm*) defines the word 'digital' as 'pertaining to data that consist of digits as well as to processes and functional units that use those data',[4] the term is often applied more broadly within NATO and the 32 national defence establishments that contribute to the Alliance, where it encompasses the integration and utilisation of digital technologies and capabilities in military operations, strategies and organisational frameworks. This includes traditional information technology (IT) and the CIS that provide core enterprise services to the Alliance, as well as the mechanisms for protecting these systems, such as cyber defence.[5] Beyond CIS, areas that are commonly included in discussions of the digital context within NATO include data standardisation, digital interoperability and relevant emerging and disruptive technologies.[6]

Additionally, 'digital' is often mentioned in the context of cyberspace and cybersecurity (see, for example, the Finnish, Polish and Swedish case studies in Annex A), but the differences between 'cyber' and 'digital' are fuzzy. Sometimes the definition of 'digital' is broader than that of 'cyber', and sometimes 'digital' is perceived as a subset of 'cyber'. At times, the terms are used interchangeably. The two are closely related. Once you possess digital technologies, which may have vulnerabilities or pose significant security risks, implementing cyber measures for their protection becomes essential. Some of the tension in the relationship between 'cyber' and 'digital' arises from the doctrinal recognition and discussion of cyber as a distinct operational domain. The box below clarifies the difference between cyber as an operational domain and cyber defence as an integral component of the digital landscape.

Box 2.1 Cyberspace vs cyber defence as an operational domain

NATO recognised cyberspace as an operational domain during the 2016 Warsaw Summit, when it acknowledged 'cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea'. The idea of cyberspace as a domain integrates cyber defence and, potentially, offence across the Alliance's three core tasks: deterrence and defence, crisis prevention and management, and cooperative security.[7] Cyber defence refers to the practical 'means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems'.[8]

4 NATOTerm Record 28685. As of 17 April 2025: https://nso.nato.int/natoterm/Web.mvc

5 NATO (2024a).

6 NATO (2024b).

7 NATO (2016).

8 NATOTerm Record 39180. As of 17 April 2025: https://nso.nato.int/natoterm/Web.mvc

Within the context of digital capability and transformation, cyber defence is, therefore, an essential component. Similarly, there are overlaps between any discussion of digital and the electromagnetic environment through which digital communications are passed; the same is true of the space domain, which depends so heavily on digital technologies and which, in turn, contributes to terrestrial digital infrastructure via provision of such services as space-based connectivity or timing signals.[9]

2.2. Digital capability and its relationship with NATO capability development

There is currently no universally agreed-upon definition of 'digital capability', including in the defence context.[10] Across government, military, industry and academic documents in this topic area, sources often use the term without defining it, often interchangeably with other terms or concepts.[11] This poses barriers to cross-sectoral collaboration at a national level, and the situation is made more complicated in an Alliance of 32 nations, where divergent definitions and priorities only throw up further barriers to cooperation and interoperability. Our research has identified two key tensions here:

1. The distinction between civilian and military interpretations of 'capability'.
2. The varying understandings of 'transformation'.

In the simplest sense, 'capability' refers to 'the ability to do something'.[12] According to the World Bank, the concept of digital capability is relatively new, and there is no single, commonly used definition. In the academic literature, it is often associated with the private sector, focusing on how companies leverage digital tools to reskill their workforce, enhance productivity, improve infrastructure and optimise products or services. In contrast, the usage of the term in the public sector has so far been more limited.[13] Definitions of 'digital capability' in the private sector typically focus on specific capabilities, such as data management, infrastructure and platforms, systems and applications and cybersecurity. However, some extend to include enablers of digital capability, such as organisational culture and leadership.[14] This broader perspective aligns more closely with the military understanding of capability, which encompasses not only specific technologies, but also the supporting elements that enhance overall effectiveness.

In NATO, on the other hand, capability refers to 'the ability to create an effect through employment of an integrated set of aspects categorized as doctrine, organization, training, materiel, leadership development, personnel, facilities and interoperability'.[15] This integrated set of aspects, which is sometimes referred to using their acronym (DOTMLPFI), underscores NATO's view of capability as a broader, system-level concept that goes far beyond hardware or software.

---

9 Shea (2025).

10 Melhem & Jacobsen (2021).

11 Schneider (2025).

12 Cambridge Dictionary (n.d.).

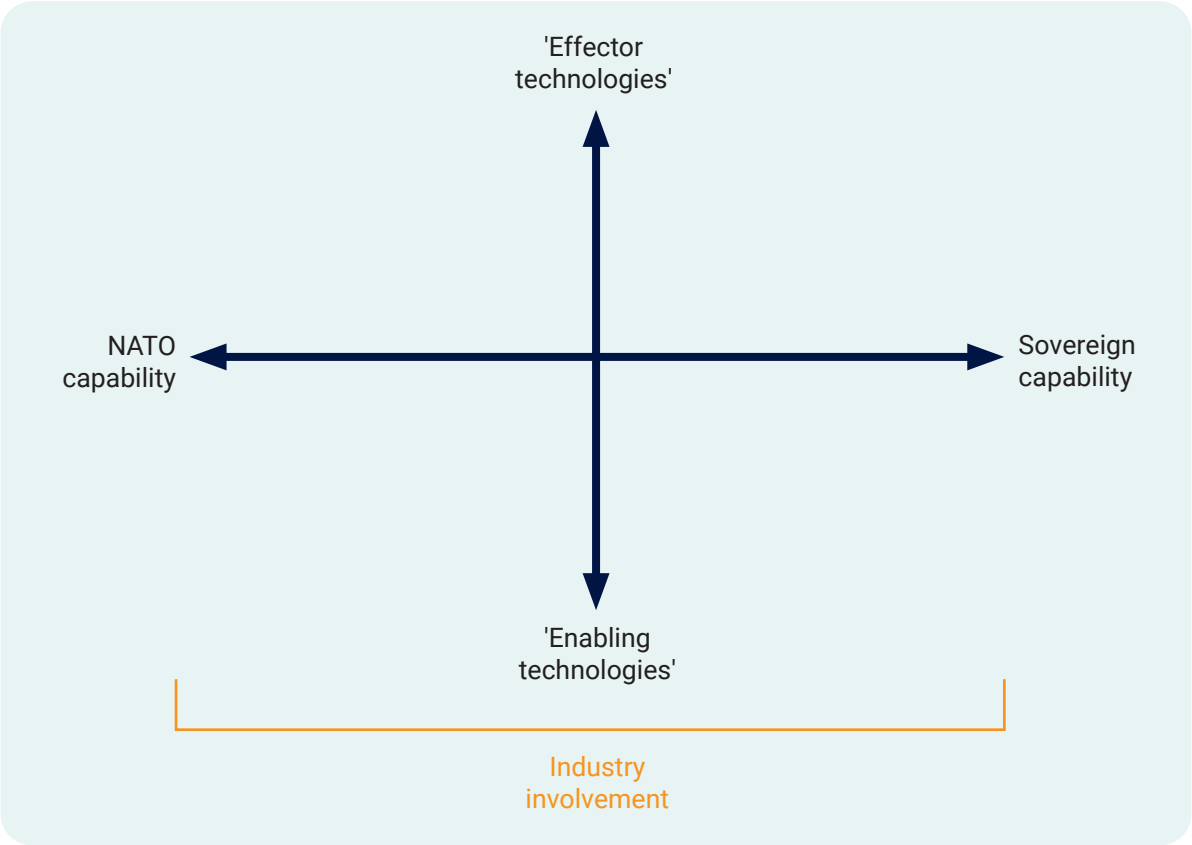
13 Melhem & Jacobsen (2021).

14 Melhem & Jacobsen (2021).

15 NATOTerm Record 27626. As of 17 April 2025: https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en

Capabilities can also take various forms, highlighting the importance of specificity when discussing digital capability within a NATO context. As illustrated below, capabilities exist on a spectrum ranging from NATO-owned and -operated capabilities to those specific to individual countries. This spectrum may also include bi- or multilateral capabilities, as well as those offered to NATO by individual Allies or groupings thereof. Additionally, capabilities can be classified along another axis, as either enabling capabilities (e.g. CIS technologies) or effector capabilities (e.g. electronic warfare). The nature of a given capability determines the involvement of various NATO stakeholders, processes and regulations. Overall, all capabilities, including digital ones, are guided by the NATO Defence Planning Process (NDPP).[16]

Figure 2.1 An illustrative digital capability spectrum



Source: RAND Europe analysis.

16 The NDPP is a structured framework designed to harmonise national and Alliance defence planning, ensuring Allies collectively develop the forces and capabilities needed to meet security objectives. It focuses on identifying requirements, setting targets and facilitating implementation through a five-step cycle, while promoting interoperability and fair burden sharing. For more information, see NATO (2022b).

While NATO does not provide a specific definition of digital capability (see Chapter 3 for a more detailed discussion of NATO's digital-related ambitions), it is evident that digital capability in an Alliance context encompasses the broader concept of capability as integrating efforts across DOTMLPFI.[17]

2.3. NATO's perspective on digital transformation

Our research also identified varying understandings of 'transformation'. As illustrated in the figure below, tensions exist between viewing capability as a time- and resource-bound effort supported by ongoing transformation (or vice-versa) or, conversely, as two continuous and mutually reinforcing processes.[18] In recent years, NATO has published strategies related to digital transformation. At the Madrid Summit, in 2022, Allies agreed on the need to strengthen NATO's technological edge. In response, NATO has published the *Digital Transformation Vision* and its accompanying *Digital Implementation Strategy* (see box below). This strategy provides a roadmap that outlines how NATO will leverage digital technologies in executing its core tasks.[19]

NATO states that the implementation effort will be a continuous, multifaceted process, spanning multiple years, addressing the three pillars of people, processes and technology.[20] Additionally, data are mentioned as a fourth and crucial enabling pillar.[21] The overall goal is to develop a workforce that is fully prepared for the digital era, to adopt flexible and agile processes, and to lead the way in the development and deployment of innovative technological solutions, such as AI, big data and quantum technologies.[22] This approach is reflected in the case study countries, which emphasise the importance of pursuing both digital literacy (i.e. achieving basic digital skills across entire organisations) and digital skills and workforce development (i.e. ensuring there are sufficient specialised knowledge, skills and ability to successfully implement and use digital technologies). The approach also contributes to NATO's strategic advantage both through direct applications in military operations and through the benefits of digital capabilities in 'back office' functions (e.g. increased productivity in procurement teams or headquarters).

NATO's vision and strategy also reflect academic understandings of digital transformation as a '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 cybersecurity and -defence policies and, critically, a mature defence-data management system'.[23] This

17 NATO (2024c).

18 As illustrated by the case study countries, which have various digital initiatives aimed at a range of developing specific capabilities, time-bound strategic investment efforts or long-term continuous transformation efforts (see Annex A).

19 NATO (2024c).

20 NATO (2025).

21 NATO (2024c).

22 NATO's ACT (2024).

23 Soare (2023).

broader conceptualisation of transformation is underscored by the case studies, particularly of Finland and Sweden, which emphasise that digital transformation involves not only acquiring new technology, but also adopting new processes, organisational structures and essential training.

Box 2.2 NATO's Digital Transformation Implementation Strategy

The *Digital Transformation Implementation Strategy* aims to transform NATO's operations by leveraging modern technologies; addressing gaps; and fostering cooperation with Allies, industry, civil society and academia.

It seeks to achieve four strategic outcomes:

1. Multi-domain operations: This refers to the ability of the Alliance to operate across all domains, with effective command and control.
2. Multi-domain interoperability: This is essential to the strategy, and processes must be modern, standardised and coherent across NATO members.
3. Enhanced situational awareness: This allows for better anticipation of risk and crisis response through access to real-time data on the multi-domain operations unfolding at any point.
4. Enhanced political consultation and data-driven decision making: These enable informed decision based on accurate data. A key mechanism to implement this vision is the Alliance Data Sharing Ecosystem, which aims to establish a norm of 'sharing interoperable data to achieve Allied objectives' so that it becomes a 'shared responsibility for Allies and the NATO Enterprise alike.'

This includes several strategic deliverables:

- Execution of Alliance digital initiatives
- Alignment of programmes
- Cultivation of digital-ready workforce and combat forces
- Development of information and communications technology (ICT) services for a data-driven Alliance
- Data-centric governance
- Rollout of a Digital Interoperability Framework
- Promotion of digital-ready processes
- Development of a Digital Backbone
- Development of an Alliance Data Sharing Ecosystem
- Cooperation with industry and academia.

Source: NATO (2025).

The *Digital Implementation Strategy* highlights three key findings regarding the concept of digital capability and its relationship to the concept of digital transformation:

1. NATO views digital capability as a key enabler for its core tasks, a topic further explored in the following chapter.
2. NATO considers digital capability to encompass, but not be limited to, the more prominent examples, such as traditional IT, CIS or cyber defence.
3. NATO perceives transformation as an ongoing and iterative process that will facilitate the development of the next generation of digital capabilities while remaining adaptable to innovation across its people, processes, technology and data.

Building a shared understanding of key terminology is essential for effective cooperation across NATO and with industry – especially in relation to industry and technology partners who may be new to defence or to the Alliance. By minimising misunderstandings and ensuring alignment among stakeholders, a common lexicon can help NATO achieve its digital ambitions and ensure innovation. Shared language and understanding of ambitions can also help build trust and strengthen long-term relationships, which are essential for standardisation and interoperability.

Chapter 3. Digital capability for achieving NATO's core tasks

NATO's *2022 Strategic Concept* outlines three core tasks: deterrence and defence, crisis prevention and management, and cooperative security.[24] The Washington Summit Declaration reinforced these tasks by highlighting NATO's role as 'the unique, essential, and indispensable transatlantic forum to consult, coordinate, and act on all matters related to our individual and collective security' in an increasingly uncertain and fragile international geopolitical environment.[25] The previous communiqués, from the Madrid and Vilnius Summits, also reaffirmed NATO's role in collective defence.[26]

Stakeholders and experts differ in their interpretations of how these core tasks should be achieved, suggesting several different priorities. Building resilience, strengthening European territorial and cyber or space defences, preserving NATO's technological edge, and improving Allied burden sharing and interoperability are all among the priorities most frequently mentioned by observers.[27] With 32 members, the Alliance can find it challenging to agree on specific strategic or geographic priorities, let alone the underpinning operational and tactical goals; observers have

24 NATO (2022a).

25 NATO (2024d).

26 NATO (2022c; 2023a).

27 See Benson (2024); NATO (2021a); Swicord (2022); Atlantic Council (n.d.).

Box 3.1 Opening paragraph of the 2024 Washington Summit Declaration

'We, the Heads of State and Government of the North Atlantic Alliance, have gathered in Washington to celebrate the 75th anniversary of our Alliance. Forged to preserve peace, NATO remains the strongest Alliance in history. We stand in unity and solidarity in the face of a brutal war of aggression on the European continent and at a critical time for our security. We reaffirm the enduring transatlantic bond between our nations. NATO remains the unique, essential, and indispensable transatlantic forum to consult, coordinate, and act on all matters related to our individual and collective security. NATO is a defensive Alliance. Our commitment to defend one another and every inch of Allied territory at all times, as enshrined in Article 5 of the Washington Treaty, is iron-clad. We will continue to ensure our collective defence against all threats and from all directions, based on a 360-degree approach, to fulfil NATO's three core tasks of deterrence and defence, crisis prevention and management, and cooperative security. We are bound together by shared values: individual liberty, human rights, democracy, and the rule of law. We adhere to international law and to the purposes and principles of the Charter of the United Nations and are committed to upholding the rules-based international order.'

Source: NATO (2024e).

also pointed out that, while NATO's core tasks are clear, agreeing on a path to implementation remains the Alliance's key challenge.[28]

Regardless of how these individual tasks for NATO are defined, however, digital capabilities remain a key enabler across the board, as illustrated by the four strategic outcomes of the *Digital Transformation Implementation Strategy* (ensuring an MDO-enabled alliance, bolstering interoperability across all domains, enhancing situational awareness, and enabling political consultation and data-driven decision making).[29] Each of these requires different technical capabilities, as well as the people, processes and data that underpin them.[30]

Digital transformation is ultimately achieved in collaboration with Allies, industry and academia. The responsibility for digital transformation within NATO involves multiple stakeholders, which can create challenges.[31] This is largely due to the complexity of the division of labour, which can lead to misunderstandings and hinder cooperation among agencies, as well as among NATO, Allied governments and militaries, and industry.[32] Some of the key barriers are incentives and sovereignty; countries generally want to retain sovereign control over as much of their sensitive digital infrastructure as possible. Additionally, aligning incentives among large commercial companies and the defence sector is often difficult, particularly when commercial entities are publicly listed and beholden to shareholders. Their interests frequently drive corporate behaviour, often regardless of national security considerations. For dual-use companies, these incentives need to align better with defence priorities, to foster effective collaboration. Table 3.1, below, outlines some of the key actors involved in this digital transformation at the NATO level.

28 Atlantic Council (n.d.).

29 NATO (2025).

30 NATO (2024c).

31 Soare (2023).

32 Soare (2023).

Table 3.1 NATO institutional stakeholders involved in digital transformation

Stakeholder	Description
Allied Command Transformation (ACT)	ACT is NATO's Warfare Development Command, focused on applying innovation to capability development to deliver more effective operational capabilities. Established in 2012, ACT's Innovation Branch is responsible for defining capability requirements and leading NATO's digital transformation to facilitate MDO.[33]
Allied Command Operations (ACO)	ACO is NATO's Strategic Warfighting Command, responsible for planning and executing all military operations to achieve Alliance objectives. It ensures interoperability across domains, integrates digital capabilities, such as enhanced situational awareness and secure communication systems, and supports NATO's wider digital transformation to improve operational effectiveness.[34]
Supreme Headquarters Allied Powers Europe (SHAPE)	SHAPE is the strategic-level headquarters of ACO, located in Mons, Belgium. It plays a critical role in digital capabilities and cyber defence, including by hosting the Cyberspace Operations Centre and the NATO Cyber Security Centre.[35]
NATO Communications and Information Agency (NCI Agency)	The NCI Agency was established in July 2012, with the aim of helping NATO maintain its technological edge. Among other areas, the NCI Agency focuses on providing NATO with technology and innovations, as well as fostering its digital transformation, which includes modernising the Alliance's Digital Backbone.[36]
Digital Policy Committee (DPC)	The DPC is a multinational NATO policy committee focused on consultation, command and control, and it is leading NATO's digital transformation. The committee is responsible for developing policies and providing guidance in these areas, as well as in interoperability standards and cyber defence.[37]
Defence Innovation Accelerator for the North Atlantic (DIANA)	DIANA is an organisation aimed at identifying and accelerating dual-use innovation capacity across NATO. Its focus areas include big data, AI, autonomy, quantum technologies, biotechnologies and human enhancement, energy and propulsion, novel materials, advanced manufacturing and aerospace.[38]
NATO Advisory Group on Emerging and Disruptive Technologies	The advisory group was established in July 2020 and comprises 12 external experts, who are responsible for advising the Alliance on optimising its innovation efforts. Additionally, it serves as an adviser to DIANA.[39]
NATO's Data and AI Review Board	The Board spearheads NATO's efforts to ensure responsible development and use of AI by helping to operationalise the principles agreed in the Alliance's AI strategy.[40]

Source: RAND Europe analysis.

33 NATO ACT (2023a).
34 NATO (2024e).
35 SHAPE NATO (n.d.).
36 NCI Agency (n.d.).
37 NATO (2024b).
38 DIANA (n.d.).
39 NATO (2024f).
40 NATO (2024f).

The remainder of this chapter therefore discusses each of NATO's core tasks described in the *2022 Strategic Concept* and how they are underpinned by the strategic outcomes described in the *Digital Transformation Implementation Strategy*.

3.1. Deterrence and defence

Deterrence refers to NATO's ability to dissuade an adversary from attacking any of the NATO members, either through the threat of punishment (e.g. military retaliation) or through denial (i.e. by making it prohibitively expensive for the adversary to achieve its goals).[41] NATO primarily achieves this through collective defence under Article 5, a commitment which is upheld through both conventional military forces and the nuclear capabilities of relevant Allies.

Demonstrating NATO members' willingness and ability to defend themselves is therefore a key cornerstone of the Alliance's deterrent effect. The ability to conduct operations across all five recognised domains is therefore critical. However, deterrence also depends on NATO Allies' demonstrated ability to operate in a concerted manner not only in the military sphere, but also across the other diplomatic, information, military, economic, financial, intelligence and law enforcement (DIME-FIL) instruments of power. The collective sanctions that many Allied nations levied on Russia following its 2022 invasion of Ukraine provide a recent example.[42] NATO also emphasises resilience and preparedness (see Section 3.2) to help Allies meet their Article 3 obligations.[43] This focus on resilience serves as an additional method of deterrence by denial, increasing the costs an adversary would expect to incur to execute a successful attack.

Digital capabilities underpin Allies' ability both to conduct military operations and to act in other areas. Further, coordination and integration among NATO members is also enabled by numerous digital capabilities. The services provided by the NCI Agency to the Alliance, which include provision of technical systems for command and control (C2), joint intelligence, surveillance and reconnaissance (ISR), as well as satellite communications, exemplify the extensive range of digital services that facilitate successful deterrence and defence.[44]

To illuminate more specific ways in which digital capabilities contribute to this task, the following section discusses MDO, which, as a key area of NATO activity, are defined as one of the four strategic outcomes sought by the *Digital Transformation Implementation Strategy*.

3.1.1. Multi-domain operations

An evolution of previous concepts for joint operations, MDO is about the more ambitious integration and coordination of activities on and off the battlefield, across all environments, including the five recognised operational domains (namely, air, land, maritime, cyber and space).[45] MDO is defined as the 'orchestration of military activities, across all domains and environments, synchronized with non-military

41 Petersen (2016).

42 Ruth (2025).

43 Article 3 of the North Atlantic Treaty obligates Allies that they 'separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack' (NATO 2009).

44 NCI Agency (n.d.a).

45 NATO ACT (2023b). See also Black & Lynch (2021); Black, et al. (2022); Spirtas (2018).

activities, to enable the Alliance to deliver converging effects at the speed of relevance'.[46]

The *Digital Transformation Implementation Strategy* recognises the importance of digital transformation to produce 'digital-ready combat forces' that can conduct MDO.[47] Elements such as situational awareness (see 3.1.2) and C2 are critical for ensuring that personnel, platforms and weapons can communicate and coordinate their activities. This might be over a wide geographical area, such as the use of satellites to facilitate communications between a Carrier Strike Group and its supporting aircraft, or focused on the deconfliction of multiple systems within a small, crowded area, such as drone swarming.[48] A number of technology areas are therefore key enablers for MDO, including communications systems, such as fifth-generation (5G) and sixth-generation (6G) telecommunications and mesh radio networks, as well as networks of sensors.[49]

The sharing of data to ensure a common operating picture and to deconflict missions in a complex operating environment is another crucial enabler.[50] AI and machine learning (ML) can also help fuse, process and analyse that data to offer decision-support tools, enabling decisions to be made with better information, at an elevated tempo.[51] To improve information sharing, decision making and C2, NATO's Military Committee issued guidance on establishing a Federated Mission Networking (FMN) as early as November 2012. The main objective of FMN is to connect forces participating in an operation to a federated mission environment, which, in turn, supports C2 and decision making through improved information sharing.[52] This includes addressing the organisational, procedural, technical, security and human aspects of connecting nations and organisations.[53] As such, the FMN is a key contribution to the Connected Forces Initiative that aims to help NATO and its partners communicate, train and operate together.[54] To further support these efforts, ACT has devoted significant effort towards delivering a secure and scalable cloud environment, intended to serve as the foundation of the future Digital Backbone (see Box 3.2).

46 NATO ACT (2022).
47 NATO (2025).
48 Kallenborn (2024).
49 Lucas, et al. (2024).
50 Ellis, et al. (2024).
51 Lucas, et al. (2024).
52 NATO ACT (n.d.a).
53 Gubbels (2023).
54 NATO C2COE (2020).

Box 3.2 The NATO Digital Backbone

One proposed solution for the challenges of MDO is the NATO Digital Backbone (NDBB). NATO documents define the NDBB as 'a federation of networks and systems that [provide] the technical means for a resilient, scalable and secure digital service continuum' and enable data-driven decision making.[55] As envisioned, it includes services both in a centralised cloud and on the network 'edge', for a wide variety of sensors, stakeholders and effectors across both traditional and non-traditional domains. The Digital Transformation Implementation Strategy further envisages the NDBB depending on a 'service-oriented architecture paradigm'.[56]

Source: NATO (2021a; 2024g).

More complex and realistic exercises are also a key enabler for MDO, enabling the testing of new concepts and technologies, the rehearsal of large-scale operations, and opportunities for Allies to become more familiar with each other's ways of working.[57] While exercises can take place in the real world, synthetic environments can offer a more low-cost, environmentally friendly means to hold exercises. The *Digital Transformation Implementation Strategy* therefore recognises synthetic environments as a key technology area for supporting effective MDO – a technology that is supported by the work of the NATO Modelling & Simulation Group.[58]

3.1.2.Enhanced situational awareness

Enhanced situational awareness is a crucial enabler of MDO. It provides a common and comprehensive view of the battlespace, thereby improving interoperability and coordination among Allies and enhancing operational effectiveness and efficiency. As described in Box 3.3, systems such as NATO's Alliance Data Sharing Ecosystem (ADSE) have been established to provide NATO commanders and forces with the necessary digital capabilities. However, these new capabilities are still evolving and developing.

Box 3.3 Alliance Data Sharing Ecosystem

In the autumn of 2024, NATO launched a new initiative called the Alliance Data Sharing Ecosystem. ADSE supports situational awareness and data-driven decision making by leveraging 'a combination of sensor networks, multiple data sources and advanced analytics to present a real-time consolidated multi-domain picture'.[59] The system is ultimately intended to share both operational and training data to help Allies better collaborate. It is hoped that, when ADSE is fully operational, it will be a force multiplier for NATO members. The pilot phase is scheduled to run to the end of 2025.

Source: NATO (2024d; 2025).

55 NATO (2024g).

56 NATO (2025).

57 Ellis, et al. (2024).

58 NATO (2024g); NATO Modelling & Simulation Group (n.d.).

59 NATO (2025).

However, enhanced situational awareness also has wider value for helping to understand and manage the wider global landscape across a variety of DIME-FIL elements.[60] Digital capabilities fundamentally underpin the ability both to collect and to cohere information for situational awareness: a wide variety of sensors, including those necessary for signals, image and measurement and signatures intelligence,[61] provide intelligence, while communications technologies allow Allies to share this picture securely. Such information can be critical in, for example, managing ladders of escalation in deterrence efforts or in understanding when the threshold of armed conflict has been breached. As the next section will also explore, situational awareness can also be a key tool for managing crisis prevention and management through early warnings, attribution or use of horizon-scanning tools to understand the environment in which an event has taken place. It can even help support an effective response: detailed longitudinal data from sensors, for example, can help identify anomalies or changes that might indicate an imminent crisis or natural disaster.[62]

3.2. Crisis prevention and management

In addition to deterring aggression and defending each another against attack, NATO Allies are also tasked with helping prevent and manage crises.[63] These can be human-made or naturally occurring, ranging from invasion to climate change to natural disaster. Regardless of the underlying cause, digital capabilities play a key role in anticipating, preventing and mitigating the effects of crisis situations.

This section delves into the underpinning strategic priority of resilience to further illuminate how this task might be performed, and the ways in which digital capabilities play a key role.

3.2.1. Crisis prevention and response

NATO contributes in several ways to crisis prevention and response, employing a comprehensive approach that integrates political, military and humanitarian tools. To prevent crises or conflict from materialising, NATO seeks to reduce tensions through diplomacy, capacity building and cooperative security measures, including training, education and defence planning with partner nations. The Alliance also maintains situational awareness and early warning systems that can assess potential or emerging crises to relevant response mechanisms.[64]

Crisis prevention and response is a collaborative effort where the Alliance works closely with key partners, such as the United Nations, the Organization for Security and Co-operation in Europe (OSCE) and the European Union (EU), as well as civilian actors, non-governmental organisations and local authorities. Digital capabilities provide key enablers for successful crisis prevention and management, including real-time data collection and analysis for situational awareness, secure communication systems between NATO and partners, and

60 For a more detailed discussion of the DIME-FIL levers, please see Rodriguez, et al. (2020).

61 For a more detailed discussion of the various types of intelligence collection disciplines, please see Federation of American Scientists (n.d.).

62 See Caves, et al. (2021) for more information about how horizon-scanning tools can be applied to prepare for and enhance resilience.

63 NATO (2022a).

64 NATO (2024e).

cyber defence to ensure resilient information-sharing mechanisms.

3.2.2. Resilience

Resilience refers to a society, organisation or individual's ability to absorb, respond to and recover from crises, which might include a natural disaster, a failure of critical infrastructure, or an armed attack. Resilience is key in ensuring the continuity of NATO's activities and, as such, it is rooted in Article 3, which requires Allies to 'maintain and develop their individual and collective capacity to resist armed attack.'[65] The requirement for much broader political, economic, technological and societal resilience in the face of hostile acts below the threshold of war is a challenge increasingly recognised by NATO since the Russian invasion of Crimea and eastern Ukraine in 2014. This refocusing began at the 2016 Warsaw Summit, with the establishment of seven baseline requirements for national resilience (see Box 3.4), which also contributed to the establishment of the joint EU-NATO Centre of Excellence for Countering Hybrid Threats in Helsinki (see Finnish case study in Annex A).[66] It was further reinforced by the *2020 Warfighting Capstone Concept*, which identified 'layered resilience' as one of the five 'development imperatives' essential for success in an era of persistent competition below the threshold of war. Additionally, the *Strengthened Resilience Commitment*, agreed upon in 2021, renewed and reinforced the commitments made at the 2016 Warsaw Summit.[67]

In 2022, NATO established the Resilience Committee, an advisory body responsible for the strategic and policy direction, planning guidance and general coordination of activities in the areas of resilience and civil preparedness.[68] Similarly, individual Allies, including the newest members, Finland and Sweden, have also adopted measures to enhance their citizens' ability to respond to crisis.[69] In reaction to the full-scale invasion of Ukraine, NATO adopted a new *Strategic Concept,* in June 2022, which is underpinned by the *Concept of Deterrence and Defence of the Euro-Atlantic Area* (DDA). The DDA considers the demands of modern warfare and the changing security environment and is described as 'purpose-driven vigilance in peacetime'.[70]

Box 3.4 NATO's baseline requirements for national resilience

1. Assured continuity of government and critical government services
2. Resilient energy supplies
3. Ability to deal effectively with uncontrolled movement of people

Source: Roepke & Thankey (2019).

65 NATO (2024h).

66 Hall & Sandeman (2022); NATO (2021).

67 Hall & Sandeman (2022); NATO (2021).

68 NATO (2022d).

69 Caves, et al. (2021).

70 Covington (2023).

As these requirements demonstrate, resilience is not only about NATO's ability to conduct operations across all domains, but also about securing its Allies' civilian infrastructure and wider societal functions in a digital age. The digital capabilities required for this task are therefore vast, from the ICT infrastructure that underpins financial markets to the radar that tracks commercial aircraft for air traffic control and from weather monitoring to civilian 5G networks. The ability to store and process data across various geographic locations, such as through cloud and edge computing, is undoubtedly an enabler of resilience; however, it also presents challenges in terms of security and dependency. As mentioned in Section 3.1.2, digital capabilities can also enable early detection of and warning about crises or natural disasters, while horizon-scanning systems can warn of possible threats before they fully manifest.

Of course, with digital capabilities underpinning critical functions, including critical national infrastructure, their ability to persist and maintain functionality under a variety of circumstances becomes a key line of effort. As NATO Secretary General Jens Stoltenberg has noted, NATO Allies might be 'more prosperous' in 'today's interconnected and digital world... but they are also... more vulnerable'.[71] Cyber attacks were, for example, a key component of Russia's strategy to weaken and disrupt Ukraine prior to invasion.[72] Russian attacks on the national infrastructure of NATO members in both cyber and physical space have persisted in an effort to limit Allies' ability to support Ukraine.[73] Digital technologies and social media platforms, similarly, expose the democratic societies of the NATO Alliance to new threats in the information environment, such as through disinformation, misinformation and hostile psychological or information operations. Growing societal reliance on space-based services and data, similarly, brings new vulnerabilities, such as to jamming, hacking or spoofing of signals or to kinetic attacks on satellites – as well as new opportunities for NATO.

The increasing reliance on the private sector for critical infrastructure and resilience, including in cyber and space, underscores an important dynamic in this context. National governments and NATO depend on private entities to provide essential services and technologies, which can enhance overall resilience but also introduce vulnerabilities. As digital capabilities play a crucial role in strengthening resilience, they simultaneously expose nations to risks associated with cyber threats and other disruptions. This dual reliance on both public and private sectors highlights the need for robust cooperation both between the civil and military sectors, as well as between NATO and private industry.

3.3. Cooperative security

The fundamental bedrock of NATO is the idea of cooperative security.[74] The ultimate example of this is the nuclear umbrella: through the NATO Nuclear Sharing Arrangements,[75] as well as national commitments from nuclear-armed powers within the Alliance, NATO members can have the protection of a nuclear umbrella without pursuing nuclear programmes of their

71 Hall & Sandeman (2022).

72 NCSC (2022); Office for Budget Responsibility (2022).

73 Jack (2024); Jones (2025).

74 NATO (2022a).

75 NATO (2022e).

own. Cooperative security is enabled by the ability of 32 different armed forces to conduct military operations together – often referred to as interoperability – as well as their respective governments' ability to reach consensus via political consultations, e.g. at the North Atlantic Council. Allies' ability to do both relies on a range of digital capabilities; these are therefore key strategic priorities for NATO's *Digital Transformation Implementation Strategy*.[76]

3.3.1. Interoperability across Allied nations

As mentioned above, NATO defines interoperability as 'the ability for Allies to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives'.[77] This, then, enables NATO to bring the mass and capabilities of all Allies to bear, rather than requiring each nation to confront challenges unilaterally. This ability to collaborate is dependent on digital capabilities for communications, information sharing, shared situational awareness and many other areas.

CIS are a critical enabler of interoperability across a range of functions, and therefore so are the digital capabilities that enable them. Integrated systems for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) are therefore key: not only must each member nation have their own systems, but Allies' systems need to be able to communicate with each another. These systems can exist across a broad range of levels of technological sophistication, from analogue radios to quantum communications. Keeping these communications and data secure and confidential requires yet more capabilities, primarily encryption; areas such as post-quantum encryption are currently areas of significant investment.

Data sharing and common storage, including for the outputs of sensors, are also key capabilities; NATO hopes to be able to provide enhanced capabilities through cloud capabilities and the NDBB. Security of digital capabilities includes both technological and people dimensions. Technologies solutions, such as encryption and an increasing emphasis on zero trust,[78] will be essential to realise NATO's ambition of secure by design.[79] Equally, comprehensive cybersecurity awareness at all levels throughout the Alliance will be required to operate these digital capabilities safely.

Interoperability presents challenges not only at the forefront of technology, but also with older digital capabilities. For instance, ensuring that radios operate on the same frequency can hinder interoperability even among legacy systems. Achieving interoperability often requires extensive cooperation, research and development, facilitated by entities such as the NATO Science and Technology Organisation, DIANA, and the NATO Centres of Excellence (COEs).[80] Additionally, the Standardisation Agreement mandates member nations to

76 NATO (2025).

77 NATO (2023b).

78 Zero trust is a security model that prioritises continuous verification of users, devices, and access requests regardless of location.

79 Secure by design seeks to build security into systems from the start through proactive measures, such as risk assessments, testing and secure coding practices.

80 NATO ACT (n.d.b).

Box 3.5 Digital Interoperability Framework

NATO's *Digital Transformation Implementation Strategy* proposes the adoption of a Digital Interoperability Framework. As envisaged, 'a common approach will be established for willing Allies to offer ICT services … digital interoperability goes beyond the development of new technologies and includes innovation acquisition, operations and sustainment of legacy products. The implementation … will contribute to the quality of data and ICT services.' The Digital Interoperability Framework was discussed at the Digital Policy Committee's Autumn Plenary in 2024; however, the policy has not yet been implemented.

Source: NATO (2024g; 2025).

implement specific standards to enhance interoperability.[81]

Standardisation is in fact a key element allowing NATO Allies to work together effectively and efficiently. The process of standardisation includes the 'development and implementation of concepts, doctrines and procedures to achieve and maintain the required levels of compatibility, interchangeability or commonality' and is overseen by a number of bodies, including the Committee for Standardisation, the NATO Standardisation Office and the NATO Standardisation Staff Group.[82] However, as will be further explored in subsequent RAND papers, such cooperation continues to be a challenge for NATO and its 32 Allies.[83] Therefore, interoperability remains an enduring challenge across the spectrum of technological sophistication. Box 3.5 discuss one way in which NATO is hoping to achieve this in the digital space.

3.3.2. Political consultation and data-driven decision making

In an alliance of 32 countries, robust mechanisms for consultation and decision making are crucial. Further, ensuring that decision making is informed by current and relevant data is critical.[84] To this end, the Alliance has, for example, established the NATO Intelligence Fusion Centre (set up in the United Kingdom [UK] in 2007) in order to 'facilitate the sharing and fusion of intelligence, contribute to filling intelligence gaps within Allied Command Operations, and to support the planning and execution of operations'.[85] In an age where disinformation and misinformation are rife, and where adversaries actively seek to undermine the Alliance observe-orient-decide-act (OODA) loop, secure digital means of communicating, verifying and securing information are important capabilities.[86] Digital decision-support tools also represent the capability for informing and speeding up decisions, through the use of AI, ML and advanced analytics.

81 NATO (2022f).

82 NATO (2022f).

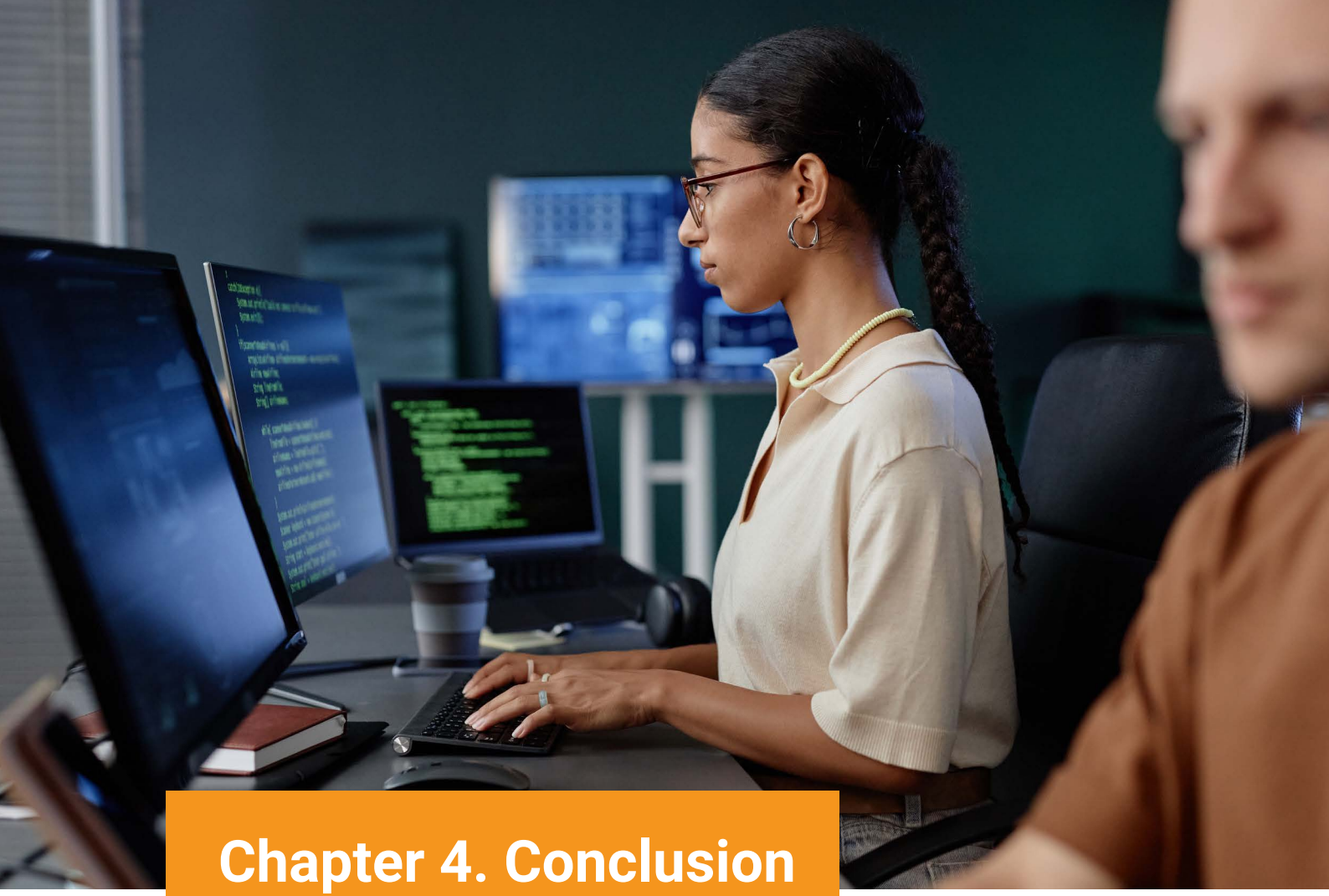
83 Paper 3 will discuss the challenges of defence industrial and scientific cooperation in more detail.

84 NATO (2025).

85 NIFC (n.d.).

86 Lucarelli, et al. (2021).

Like several other strategic outcomes discussed here, persistent sharing and access to data pose technical challenges. Cloud systems and edge computing can help address some of these issues. The proposed NDBB and ADSE systems mentioned earlier are potential solutions for NATO in this regard. However, the effort to improve information sharing is not solely focused on cutting-edge capabilities; ensuring the continued functionality and security of legacy systems, such as telephones and radios, is also a critical enabler in this area.



Chapter 4. Conclusion and next steps

This paper has set out to explore the concept of digital capability and whether and how this differs from digital transformation.

Our analysis reveals a lack of universally accepted definitions for 'digital', 'digital capability' and 'digital transformation', particularly within defence. These terms are often used interchangeably, leading to tensions, especially between civilian or industry contexts and NATO contexts.

In NATO, the term 'digital' is used in a broad way, encompassing the integration of digital technologies in military operations and organisational frameworks. This includes traditional IT and CIS and extends to cyber defence, data standardisation, digital interoperability and emerging technologies. It comprises both enabling and effector capabilities, with applications both to military operations and to 'back office' functions.

NATO refers to capability as 'the ability to create an effect through employment of an integrated set of aspects categorized as doctrine, organization, training, materiel, leadership development, personnel, facilities, and interoperability'. This DOTMLFPI approach emphasises NATO's view of capability as a broader, system-level concept. Within the Alliance context, it is also important to distinguish between NATO-owned and -operated capabilities and national capabilities specific to individual countries, as well as to recognise the growing role of commercial suppliers in maintaining and deploying digital capabilities. This presents a more complex context for integration and interoperability

than more traditional domains or non-digital capability areas (e.g. given the software-driven nature of many digital technologies, which necessitates much faster capability upgrade cycles and feedback loops from end users back to industry). Digital capability is a key enabler for NATO's core tasks.

The understanding of the concept of digital transformation is also varied, with some viewing it as time- and resource-bound, and others seeing it as a continuous process that complements digital capabilities. NATO's *Digital Transformation Vision* and accompanying *Digital Implementation Strategy* emphasise the latter approach, with transformation focused on ongoing and long-term efforts. Digital transformation within NATO is an ongoing and iterative process that will facilitate the development of the next generation of digital capabilities while remaining adaptable to innovation across its people, processes, technology and data.

Our main recommendation is therefore to foster shared understanding of these terms, which is vital for effective cooperation across NATO and with industry and the science and technology community, particularly with partners new to working in defence. A common lexicon can minimise misunderstandings, align stakeholders and foster trust, all essential for standardisation and interoperability, thereby aiding NATO in achieving its digital ambitions.

The paper has also explored the role of digital capabilities in the context of NATO's core tasks. The Alliance continues to be the foremost pillar of transatlantic security and an important element of the global international order. For NATO to fulfil its core tasks, it will need to achieve the desired strategic objectives as outlined in the *Digital Transformation Implementation Strategy*. Table 4.1, below, illustrates how digital capabilities may contribute to NATO's core tasks.

This is the first in a series of three papers exploring the evolving role of digital capabilities in the NATO Alliance. The second paper will cover implications and enablers of effective digital capability management and explore:

- Barriers and enablers to effective digital capability development in NATO
- Possible implications of digital capability development for defence spending across NATO
- Possible implications of underinvestment in digital capabilities

The third paper will cover the topic of interoperability in the digital environment and explore:

- Opportunities and challenges for fostering greater interoperability in the digital environment (particularly considering growing demands for digital sovereignty among NATO Allies)
- Implications of fostering digital interoperability for European strategic autonomy, the European defence industry and defence industrial cooperation within NATO.

Table 4.1 Illustrative example of ways digital capability contributes to NATO core tasks

Core task	Ways digital capabilities can enable the core task
Deterrence and defence	Digital capabilities enhance NATO's collective defence by facilitating military operations and coordination among Allies through services such as C4ISR and through: • Multi-domain operations (MDO): Technologies, such as advanced communications systems and artificial intelligence (AI), enable 'digital-ready combat forces' to conduct MDO, supporting real-time data sharing and situational awareness for synchronised military and non-military activities. • Enhanced situational awareness: Systems such as NATO's Alliance Data Sharing Ecosystem improve interoperability and operational effectiveness by providing a comprehensive view of the battlespace and facilitating real-time data sharing.
Crisis prevention and management	Digital technologies enhance resilience by enabling early detection and response to crises, ensuring continuity of operations and effective management of critical infrastructure.
Cooperative security	Digital capabilities support interoperability among Allies, allowing for effective joint military operations through secure communication systems and data-sharing platforms via: • Interoperability: Robust digital communication and information systems, along with standardisation efforts, are essential for achieving seamless collaboration across various technological levels. • Political consultation and data-driven decision making: Digital tools, such as those of the NATO Intelligence Fusion Centre or Supreme Headquarters Allied Powers Europe (SHAPE), facilitate secure sharing and analysis of intelligence, ensuring informed and timely decision making.

Source: RAND Europe analysis.

Annex A. Selected national approaches within NATO

This annex dives into selected Allies' approaches to civilian and military digital capability development.[87] Case studies are used to illustrate how individual nations understand digital capabilities in their national context, what outcomes they have set out to achieve in terms of digital capability development, where their priorities lie and how they have linked digital capabilities to wider strategic objectives. This annex covers four country case studies: Estonia, Finland, Poland and Sweden.

A.1. Estonia

Despite its small size and population, Estonia is seen as one of the biggest players in the field of digital capabilities and cybersecurity, often cited as a prime example of successful digitalisation efforts.[88] According to Toomas Ilves, President of Estonia between 2006 and 2016, digitalisation was the ultimate key to economic and social national development after Estonia gained independence from the Soviet Union in 1991.[89] The country was able to take advantage of the opportunity presented by the independence, building successful e-government infrastructure on a platform for decentralised databases and data exchange known as X-Road, and a compulsory national digital identification. However, Estonia's digital success is mainly centred around the digital public service infrastructure, with other digital offerings lagging.[90] This helps to explain why the country does not rank as high in overall digital transformation indices, and why these overall indices might not be the most reliable indicator of digitalisation.[91]

To further advance Estonia's economy, state and society through digital technology, the country adopted the *Estonian Digital Agenda 2030,* in 2021. The development plan is centred around three main areas: digital state, connectivity and cybersecurity. The document also underpins Estonia's 2023 *European Digital Decade Strategic Roadmap*, which aims to

87 The case study countries represent a selection of Allies known for their digital capabilities and Allies that have recently increased their investment in this space. The selection of case studies was discussed and agreed with Microsoft.

88 Complex Discovery (2025).

89 Ilves (2024).

90 Kattel & Mergel (2019).

91 Kattel & Mergel (2019); Jermalavičius (2024).

achieve EU's digital targets set for 2030.[92] The main goals of the Roadmap are digital skills, digital infrastructure, digitalisation of the public sector and digitalisation of business.[93] Currently, Estonia's strength lies in the digitalisation of public services, the number of ICT specialists and the level of digital skills among Estonia's population. In contrast, the country is currently lacking in connectivity infrastructure, as well as in digitalisation of small and medium-sized enterprises, which remains behind the EU average.[94]

A.1.1. Digital capabilities and defence

Estonia's high level of digitalisation helped the country transform itself into a major player in the field of cybersecurity and an important NATO ally. With over 99 per cent of public services available online, Estonia must respond to a large number of cybersecurity challenges. In 2024, the Estonian Information System Authority recorded 6,515 impactful cyber incidents, nearly twice as many as in 2023, with global crises, including the wars in Ukraine and the Gaza Strip, adding to the uptick in cyber incidents.[95] Estonia's experience with cyber attacks has shaped it into a key player in the field of cybersecurity, with major attacks in 2007 prompting the country to significantly strengthen its national cyber security. In 2008, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established in Tallinn, and CCDCOE now has the most member states of all of NATO's 28 centres of excellence.[96] CCDCOE is, among other things, responsible for the publication of the *Tallinn Manual*, a resource for legal advisers and policy experts dealing with cyber issues, and it hosts the annual Locked Shields exercise to bring together cyber experts from across the Alliance.[97]

Domestically, cyber resilience has become a key focus of the government, as exemplified in the Estonian Cyber Defence League. The volunteer organisation, which is the cyber defence unit of the Estonian Defence League, a voluntary national defence organisation operating within the jurisdiction of the Ministry of Defence, was established in reaction to the 2007 cyber attacks.[98] It is a national collaboration model for cyber security professionals who are members of a voluntary paramilitary national defence organisation, and as such represent an innovative model for the involvement of volunteers in national cyber defence.[99] This approach helps Estonia bring together skills from across the private and the public sectors, enabling the country to draw on these in times of crisis. In addition to increasing Estonia's cyber resilience, this approach also helps mitigate the inability

92 The *European Digital Decade Strategic Roadmap* is an EU policy programme which sets up an annual cooperation cycle to achieve common objectives and targets through to 2030, resting on the four pillars of skills, infrastructures, business and government. The cooperation mechanism involves Member States and the Commission, which developed EU-level projected trajectories for the attainment of the digital targets set under the policy programme. For more detail, see European Commission (n.d.).

93 Estonian Ministry of Economic Affairs and Communications (2023).

94 European Commission (2024a).

95 E-Estonia (2024); The Baltic Times (2025).

96 French Institute for Higher National Defence Studies (n.d.).

97 CCDCOE (n.d.a; n.d.b).

98 Estonian Defence League (n.d.).

99 Kaska, et al. (2013).

to recruit sufficient workers that the field of cybersecurity often faces.[100]

In March 2025, Estonia's Ministry of Defence published its first *Defence AI Development Strategy*. The strategy aims to increase Estonia's defence AI capabilities. To fulfil the objectives of the strategy, the *National Defence Development Plan* for the period 2026–2035 is envisioned to dedicate 30–50 per cent of the annual research and development (R&D) budget to developing AI with defence applications.[101] A key element of the strategy is the building of a digital infrastructure for the Estonian Defence Forces in order to enable more expansive use of AI solutions and to drive interoperability among Estonian defence institutions and between Estonia and its NATO Allies.

A.2. Finland

Finland has invested heavily in digitalisation, as reflected in its high rankings and by the existence of several policy and strategic documents focused on the area. As the former Director of Public Sector ICT stated: 'Finland continually ranks as number one in public sector digitalisation, as indicated by the European Commission's Digital Economy and Society Index (DESI)'.[102] Finland's key strengths include a highly digitally literate population – a literacy that is supported and enabled by open training in areas such as cyber security – and high levels of digitalisation among small and medium-sized enterprises. Finland is seeking to improve digital public services linked to e-Health and electronic identification (e-ID), as well as address its below–EU average deployment of gigabit networks across the country.[103]

The importance of digitalisation is reflected in several strategic policy documents. For example, Finland's *National Roadmap*, which was published in 2024 and underpins the EU's *Digital Decade Policy Programme 2030*, focuses such key targets as competence, digital infrastructure, businesses and public services.[104] The planned measures for reaching the targets include promoting digital skills, media literacy and digital self-cultivation; developing educational pathways for ICT experts; promoting broadband investment; and supporting investment in R&D.[105] To further support its digitalisation efforts, the country published the *Digital Finland Framework*, which is aimed at achieving effective coordination of sustainable digital transformation in Finland.[106] To achieve the digital transformation, Finland is looking to create a funding instrument to support innovation ecosystems, create accelerator mechanisms to increase technology adaptation, focus on research–business cooperation to develop digital skills, ensure public funding for and investment in digital transformation, and ensure international collaboration. More recently, in December 2024, the ministerial working group on reforming society decided to update the *Digital Compass* implementation plan. The *Digital Compass* is a tool guiding Finland's digital transformation,

100 Digital Front Lines (2023).

101 Estonian Ministry of Defence (2025).

102 Karjalainen (2020).

103 European Commission (2024b).

104 Finnish Government (2024a).

105 For detailed overview of planned measures and funding, see Finnish Government (2024a).

106 Business Finland (n.d.).

with core objectives focused on competence, infrastructure, public services and business.[107]

A.2.2. Digital capabilities and defence

Digital capabilities and information management were recognised as one of essential enablers for defence in Finland's 2021 *Defence Report*.[108] The document acknowledges the effects of digital technologies on the security and operating environments, which, in turn, highlights the importance of maintaining and developing legislation, skills and technological capabilities. The overarching objective of the digitalisation of the Finnish Defence Forces is 'to manage risks associated with emerging technologies, take advantage of opportunities, optimise activities, create new services, activities and knowledge, develop new abilities, and to be involved in national decisions,' with particular focus on the development of AI.[109] To this end, the country implemented the Defence Force's digitalisation strategy and digitalisation programme, which ran from 2021 to 2024.[110]

Finland is looking to leverage the relationship between the civilian and the military spheres, as embodied in the so-called Digital Defence Ecosystem. The Digital Defence Ecosystem is a network of civilian dual-use technology companies, military technology companies and research institutes that seek to develop new digital defence solutions.[111] The ecosystem is coordinated by the Finnish programme management company XD Solutions and has been joined by 37 organisations, including Saab, Nokia and Tampere University. The endeavour is a part of what the network describes as a phenomenon of 'new defence', which sees private companies increasingly involved in developing technologies for defence applications, similarly to how private companies now explore space technology in support of such governmental organisations as the European Space Agency and the United States' National Aeronautics and Space Administration (NASA).[112]

To further strengthen its digital and cybersecurity defence, Finland launched the *Digital Resilience Programme,* in August 2024. The programme, spearheaded by Business Finland, the country's official government agency for trade and investment promotion, will run until 2028 and will allocate €100 million to innovation, research and international partnerships. Aiming to position Finland as a leader in digital security, the Digital Resilience Programme focuses on the following key areas 'enhancing digital defence capabilities, promoting quantum-safe cryptology, and ensuring the security of critical communications.'[113] International cooperation is a central tenet of the programme, particularly in the context of growing European collaboration and the cooperation between Finland and its NATO Allies. The country's capital is also the home of the European Centre of Excellence for Countering Hybrid Threats. Established in 2017, this COE's purpose is to strengthen cooperation between the EU and NATO to help the two organisations and

107 Finnish Government (2024b).
108 Finnish Government (2021).
109 Finnish Government (2021); Järvinen (2024).
110 Finnish Defence Forces (n.d.).
111 Digital Defence Ecosystem (n.d.).
112 Digital Defence Ecosystem (n.d.).
113 Granlycke (2024).

the member states counter hybrid threats. This is done by encouraging strategic-level dialogue, conducting research and analysis into hybrid threats, and developing doctrine and conducting training and exercises.[114]

The changing security environment also prompted Finland to publish a revised *Cyber Security Strategy* for the period 2024–2035. The document identifies cybersecurity as a part of Finland's comprehensive security and digitalising society, and the importance of cybersecurity was further underscored by geopolitical shifts and changes in Finland's security environment. The strategy rests on four pillars: competence, technology and research; development and innovation; preparedness, cooperation and response; and countermeasures.[115] However, the document acknowledges that the current annual spending, of approximately €300 million, on cybersecurity is insufficient for responding to the evolving security environment.

Besides insufficient funding, Finland faces further challenges stemming from its accession to NATO, primarily integration and interoperability. As outlined in the *2024 Government Defence Report*, the Finnish Defence Forces now focus on 'integrating with NATO by developing its information management processes, by implementing the data and communications technology solutions necessary for preparation and decision-making processes and by modernising its facilities'.[116] The ambition is to fully apply NATO's requirements and standards on information management and security in national development efforts.

A.3. Poland

While Poland remains below the EU average level of digitalisation according to the *eGovernment Benchmark* 2024 insight report, it recorded significant progress in the period 2022–2023.[117] It embarked on a significant effort to achieve the *Digital Decade* objectives and targets set out by the EU, an effort that is underpinned by a total budget of some €12.4 billion, or 1.6 per cent of its gross domestic product (GDP).[118] Poland's strengths include a high-gigabit connectivity coverage and the digitalisation of small and medium-sized enterprises, the pace of which is six times higher than in the EU.[119] However, adoption of advanced digital technologies, except for the cloud, remains low compared with the EU average, as does the share of the population which possesses at least basic digital skills.[120]

To bolster digitalisation, Poland published its first digitalisation strategy, in October 2024, covering the period until 2035. According to the Minister of Digital Affairs, Krzysztof Gawkowski, the changing landscape of national security, trends and challenges in technology, and the economy are some of the key drivers of investment in digitalisation.[121] The main goal of the document, which is the first strategy of this kind in Poland, is to improve the quality of

114 EEAS (2017).
115 Finnish Prime Minister's Office (2024).
116 Finnish Ministry of Defence (2024).
117 Ptak (2024); Capgemini, et al. (2024).
118 European Commission (2024c).
119 European Commission (2024c).
120 European Commission (2024c).
121 Polish Ministry of Digital Affairs (2024).

life of the population, with some key targets including universal access to high-speed internet, the complete digital transformation of public services, the development of quantum computing capabilities, the creation of a robust AI ecosystem, and enhanced cybersecurity infrastructure.[122] To support this effort, Poland is planning on spending 5 per cent of its GDP on digitalisation by 2035.[123]

The increased focus on digitalisation, alongside cybersecurity, is also reflected in Poland's 6-month programme for its EU Council presidency, which began on 1 January 2025. The main strategic areas are cybersecurity, new technologies and cyber diplomacy. More specifically, Poland focuses its efforts on the *Digital Networks Act*, EU's AI strategy and workplace automation and protection, as well as a range of cybersecurity priorities, including a progress report on the *EU Cybersecurity Act*, an update to the European Commission's (EC) 2017 *Cyber Blueprint*, and the *Digital Operational Resilience Act*.[124]

A.3.1. Digital capabilities and defence

The increased focus on digital capabilities and digital security comes in the context of a deteriorating security environment and an increase in hybrid threats. In fact, Poland has become the most attacked country in the world, with an average of 1000 cyber attacks on organisations per week.[125] The number of attacks rose significantly following the Russian full-scale invasion of Ukraine in 2022. For example, in June 2024, the Polish news agency Polska Agencja Prasowa was targeted by a suspected Russian cyber attack, which saw the publishing of a false article about military mobilisation on the agency's website. In response, the Digitalisation Minister announced additional spending of €704 million to boost Poland's cybersecurity.[126]

As a result, cybersecurity has emerged as a key priority in Poland, as reflected in its strategic goals for the EU presidency. More specifically, Poland's strategic objectives for the presidency include cybersecurity, new technologies and cyber diplomacy.[127] Focusing on cyber resilience, Warsaw hosted a meeting of EU ministers responsible for cybersecurity, on 5 March 2025, which was entirely dedicated to cybersecurity and resulted in the adoption of the *Warsaw Call*.[128] The document stressed the need to strengthen resilience, cybersecurity and cyber defence in the light of geopolitical changes and ongoing Russian aggression against Ukraine. To pursue preparedness and cooperation, the ministers agreed to 13

122 Decent Cybersecurity (2024a).

123 Polish Ministry of Digital Affairs (2024).

124 Alexe (2025). The EU Digital Networks Act aims to change the EU telecommunications regulations to address the evolving digital landscape, with emphasis on the development of digital network infrastructures. The Act also aims to create a level playing field to allow new business models to emerge in order to foster innovation. For more information, see Digital Networks Act (n.d.). The EU Cybersecurity Act strengthens the EU Agency for cybersecurity, which is mandated to increase cooperation among the Member States at the EU level, and introduced a new EU-wide cybersecurity certification framework for ICT products, services and processes. For more information, see European Commission (2025a). The EU Digital Operational Resilience Act seeks to strengthen cybersecurity and resilience of financial companies such as banks, insurance companies and investment firms. For more information, see EIOPA (n.d.). The EU Strategy on AI aims to position the bloc as a world-class hub for AI while ensuring the responsible use of AI that is human-centric and trustworthy. For more information, see European Commission (2025b).

125 International Trade Administration (2024a).

126 Reuters (2024).

127 International Trade Administration (2024b).

128 Polish Presidency Council of the European Union (2025).

points, which include enhancing cooperation and information exchange on cybersecurity, harmonising investments in cybersecurity, and devising a roadmap on new technologies impacting cybersecurity.[129]

Beyond security, the Polish Ministry of Defence also published an *AI Strategy* for the period 2024–2039, one of the first Polish government documents to address the implementation of new technologies. The strategy aims to put in place conditions for the responsible development, implementation and use of AI and should help Poland achieve technological advantage over potential adversaries.[130] The key implementations include autonomous systems, intelligence and reconnaissance, logistics and support, and cybersecurity. An integral part of the strategy is the establishment of the Artificial Intelligence Implementation Centre within Poland's Cyberspace Defence Forces, which will seek to advance and integrate AI across all operational domains of the Polish armed forces.[131]

In addition to AI, Poland is making progress in attaining other technologies that will help it leverage the benefits of digitalisation. For example, in December 2024, it was reported that the country's prototype quantum computer for military and special IT applications was at an advanced stage, with the spokesperson of Polish Cyberspace Defence Forces stating that the project was expected to be completed by the end of 2025.[132] That same month, Poland's Ministry of National Defence declared initial operational capability for the first Integrated Battle Command System (IBCS)-enabled battery of its medium-range defence programme. IBCS is a C2 system with a network-enabled, modular, open and scalable architecture, and is a foundational element for enabling MDO.[133]

A.4. Sweden

Sweden is considered a leader in digital innovation, boasting a robust infrastructure and a supportive regulatory environment, which put it at the forefront of digitisation. The country has one of the most advanced information and communication infrastructures in the world, which is leveraged by a population highly proficient in using digital tools, thanks to Sweden's commitment to digital literacy.[134] In addition to the strong connectivity infrastructure, the business environment in Sweden is another of the country's strengths, as it is conducive to innovation and has good access to financing.[135] In terms of weaknesses, Sweden is trying to increase accessibility of e-ID and is currently lagging the EU average in online access to electronic health journals.[136]

Sweden's strategic goals to be achieved by 2030 are set out in the government's roadmap for the *Digital Decade*. This document outlines a range of measures to be achieved, as well as the key challenge that needs to be overcome, namely, the difficulty of recruiting ICT specialists, which remains despite the

129 Polish Ministry of Digital Affairs (2025).
130 Polish Ministry of National Defence (2024).
131 Army Technology (2025).
132 Choucair (2025).
133 Northrop Grumman (2024).
134 International Trade Administration (2024c).
135 European Commission (2024d).
136 European Commission (2024d).

population's high level of digital literacy.[137] In January 2023, Sweden launched the Digital Transformation Infrastructure Plan, which should help the country drive digital transformation further and help the population achieve the necessary digital skills. The 4-year plan is underpinned by investment worth €1 billion and prioritises the areas of government and public services, such as education, transportation and healthcare.[138]

A.4.1. Digital capabilities and defence

Sweden is well positioned to translate successful digitalisation efforts from civilian to military settings thanks to the close relationship between the two. The country has a long experience with the concept of total defence, which involves the whole of society and consists of both military and civil defence, both of which have been strengthened further since 2015 due to the Russian invasion of Crimea the year before.[139] Aiming to strengthen societal resilience, the concept has collaborative civil–military interactions at its core.[140] As a result, the close relationship among civil society, the private sector, and governmental and military organisations is conducive to innovation, which can feed from the civilian industry into the military community.[141]

The focus on civil–military collaboration is reflected in the recently adopted *Total Defence Bill* for the period 2025–2030, which substantially reinforces Sweden's total defence. The government is also working to reorganise the country's National Cybersecurity Centre, with the aim of establishing a stronger national structure and a clear hub for cybersecurity work.[142] It also recognised the importance of resilience by expanding its Think Secure campaign, which promotes more secure digital activity in society.[143] To further its defence, the government is currently working on a national cybersecurity strategy, which will replace the one published in 2017 and will provide a new direction and an action plan.

In December 2024, the Swedish government published *Sweden in a Digital World*, which presents a strategy for the country's security policy on cyber and digital issues. The document highlights the changing international system, in which cyber and digital issues play an essential role, demonstrating 'that technology, economics, democracy and security are increasingly intertwined in international relations'.[144] The strategy was also designed to be mutually reinforcing with the upcoming cybersecurity strategy, which will be published later this year.

To further take advantage of digitalisation and technological innovation, the Swedish Armed Forces (SAF) started a programme focused on civil–military synergies in research and development, in June 2024.[145] This is done in collaboration with the Swedish Governmental Agency for Innovation Systems, known as Vinnova, with a focus on such areas as

137 Krasavina (2024).
138 O'Dwyer (2023).
139 Government Offices of Sweden (n.d.a).
140 Tillberg, et al. (2025).
141 Finlan (2024).
142 Government Offices of Sweden (n.d.b).
143 Government Offices of Sweden (n.d.b); Internet Stiftelsen (n.d.).
144 Swedish Ministry of Foreign Affairs (2024).
145 Vinnova (2024).

AI, quantum technology and autonomous systems. The worsening security environment has shown the importance of having defence that is capable of innovating quickly, with the SAF stating that 'to successfully meet this change, partnership between the public and private sectors is needed, particularly with the aim of bringing together academia, industry and government in a triple helix model of innovation'.[146] The innovation programme for civilian–military synergies will be able to build on existing efforts, such as the advanced digitalisation programme, for which the government earmarked €46.3 million per year starting in 2024.[147]

Sweden is currently developing the digital infrastructure for C2 and cooperation for the SAF, known as Combat Support System (known by the Swedish acronym LSS) Mark. The effort is driven by cooperation between the Swedish Defence Materiel Administration (known by the Swedish acronym FMV) and Saab, which will be responsible for integration, design and development of existing and future versions of the system.[148] The programme, which was first envisaged in 2015 but underwent significant changes due to the changing security environment and Sweden's accession to NATO, aims to replace all the radios and C2 systems of SAF's ground components. Interoperability with NATO's FMN framework is an important factor in the development of the system.[149]

Despite significant efforts, Sweden continues to face multiple challenges. Most notably, these include the recent accession to NATO, which requires SAF to enhance its interoperability with the Alliance, and improving the ability of the existing force structure to rapidly adopt technological innovations.[150] As a result, there is a need for change in many areas, such as doctrine, handbooks and manuals, especially in preparation for aligning with MDO.[151] The challenges highlight the fact that digital transformation is not only about getting new technology, but also about adopting new processes, organisational structures and necessary training. To address the challenges, there is a strong focus on integration with NATO in Sweden's new defence bill, alongside prioritisation of technological innovation and cyber security.[152] For example, Sweden is enhancing its command capability to further develop interoperability with NATO and strengthening its capability to support Allied operations as a host nation.[153]

146 Swedish Ministry of Defence (2024).
147 Swedish Ministry of Defence (2024).
148 Saab (2024).
149 Ebbutt (2025).
150 Lindfors, et al. (2024).
151 Lindfors, et al. (2024).
152 Khorrami (2024).
153 Government Offices of Sweden (n.d.a).

References

Alexe, Paula. 2025. 'Poland Sets Out Digital Priorities for the Next Six Months.' *Bird&Bird.* 23 January. As of 27 March 2025: https://www.twobirds.com/en/insights/2025/poland-sets-out-digital-priorities-for-the-next-six-months.

Army Technology. 2025. 'Poland to Strengthen Security with New AI Implementation Centre.' March 4. As of 9 April 2025: https://www.army-technology.com/news/poland-ai-implementation-center/

Aronsson, Lisa & Brett Swaney. 2023. 'Priorities for NATO Partnerships in an Era of Strategic Competition'. *Institute for National Strategic Studies Strategic Perspectives* 40, 11 July. As of 29 March 2025: https://inss.ndu.edu/Media/News/Article/3455040/priorities-for-nato-partnerships-in-an-era-of-strategic-competition/

Atlantic Council. n.d. 'Scowcroft Strategy Scorecard.' *Atlantic Council.* As of 29 March 2025: https://www.atlanticcouncil.org/content-series/scorecard/scowcroft-strategy-scorecard-natos-strategic-concept/

Benson, Robert. 2024. 'Shaping NATO's Future: 5 Key Priorities for Washington to Build On After the 75th NATO Summit.' *Center for American Progress*, 11 July. As of 29 March 2025: https://www.americanprogress.org/article/shaping-natos-future-5-key-priorities-for-washington-to-build-on-after-the-75th-nato-summit/

Black, James & Alice Lynch. 2021. *Cyber Threats to NATO from a Multi-Domain Perspective.* Cooperative Cyber Defence Centre of Excellence. EP-68434. As of 9 April 2025: https://www.rand.org/pubs/external_publications/EP68434.html

Black, James, Alice Lynch, Kristian Gustafson, David Blagden, Pauline Paillé & Fiona Quimbre. 2022. *Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea.* Santa Monica, Calif.: RAND Corporation. RR-A528-1. As of April 9, 2025: https://www.rand.org/pubs/research_reports/RRA528-1.html

Business Finland. n.d. *Digital Finland Framework: Framework for Turning Digital Transformation to Solutions to Grand Challenges.* Helsinki: Ministry of Economic and Employment of Finland/Business Finland/VTT Research. As of 27 March 2025: https://www.businessfinland.fi/globalassets/julkaisut/digital-finland-framework.pdf

Cambridge Dictionary. n.d. 'Capability.' As of 9 April 2025: https://dictionary.cambridge.org/dictionary/english/capability

Capgemini, Sogeti, IDC & Politecnico di Milano. 2024. *eGovernment Benchmark 2024 Insight Report.* Brussels: European Commission Directorate-General for Communications Networks, Content and Technology. As of 9 April 2025: https://www.capgemini.com/wp-content/uploads/2024/07/eGovernment-Report-2024.pdf

Caves, Ben, Rebecca Lucas, Livia Dewaele, Julia Muravska, Chris Wragg, Tom Spence, Zudik Hernandez, Anna Knack & James Black. 2021. *Enhancing Defence's Contribution to Societal Resilience in the UK: Lessons from International Approaches*. Santa Monica, Calif.: RAND Corporation. RR-A1113-1. As of 29 March 2025: https://www.rand.org/pubs/research_reports/RRA1113-1.html

CCDCOE (Cooperative Cyber Defence Centre of Excellence). n.d.a. 'Locked Shields.' As of 27 March 2025: https://ccdcoe.org/locked-shields/

———. n.d.b. 'The Tallinn Manual.' As of 27 March 2025: https://ccdcoe.org/research/tallinn-manual/

Choucair, Cierra. 2025. 'Poland Advances Development of Military Quantum Computer Prototype, Source Says.' *Quantum Insider.* 30 January. As of 27 March 2025: https://thequantuminsider.com/2025/01/30/poland-advances-development-of-military-quantum-computer-prototype-source-says/

Complex Discovery. 2025. 'Finally 100% Digital: Estonia's 30-Year Journey from the USSR to e-Estonia.' 31 January. As of 4 April 2025: https://complexdiscovery.com/finally-100-digital-estonias-30-year-journey-from-the-ussr-to-e-estonia/

Covington, Stephen R. 2023. 'NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA).' *Belfer Center for Science and International Affairs*. 2 August. As of 9 April 2025: https://www.belfercenter.org/publication/natos-concept-deterrence-and-defence-euro-atlantic-area-dda#in-this-section-nav-2

Decent Cybersecurity. 2024a. 'Poland Unveils Landmark Digital Strategy 2035: A Comprehensive Roadmap for Digital Transformation.' 20 November. As of 27 March 2025: https://decentcybersecurity.eu/poland-unveils-landmark-digital-strategy-2035-a-comprehensive-roadmap-for-digital-transformation/

Defence Innovation Accelerator for the North Atlantic. n.d. 'DIANA.' As of 9 April 2025: https://www.diana.nato.int/index.html

Digital Defence Ecosystem. n.d. 'Digital Defence Ecosystem'. As of 27 March 2025: https://www.digitaldefence.fi/

Digital Front Lines. 2023. 'Lessons from Estonia's Whole-of-Society Approach to Cyber Defense: A Q&A with Hanno Pevkur.' August 31. As of 27 March 2025: https://digitalfrontlines.io/2023/08/31/lessons-from-estonias-whole-of-society-approach-to-cyber-defense/

Digital Networks Act. n.d. 'Digital Networks Act (DNA): Updates.' As of 9 April 2025: https://www.digital-networks-act.com/

Ebbutt, Giles. 2025. 'Sweden's Land Digitisation Programme Ramps Up, C2 Application Evolving.' *Jane's.* As of 27 March 2025: https://customer.janes.com/display/BSP_84194-JDW

E-Estonia. 2024. 'A Year of Advanced Threats and Global Tensions: Estonia's Cyber Security Scene in 2023.' 9 April. As of 27 March 2025: https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats/

Ellis, Conlan, Rebecca Lucas, Ben Fawkes, Martin Robson, Alan Brown, Edward Keedwell & James Black. 2024. *Command and Control in the Future: Concept Paper 3 – Conceptualising C2 as a Capability*. Santa Monica, Calif.: RAND Corporation. RR-A2476-3. As of 29 March 2025: https://www.rand.org/pubs/research_reports/RRA2476-3.html

Estonian Defence League. n.d. 'Estonian Defence League.' As of 9 April 2025: https://www.kaitseliit.ee/en/edl

Estonian Ministry of Defence. 2025. *Defence Artificial Intelligence strategy for Estonia.* Tallinn: Ministry of Defence. As of 27 March 2025: https://kaitseministeerium.ee/sites/default/files/defence_artificial_intelligence_strategy_for_estonia.pdf#page=8.10

———. 2023. *European Digital Decade Strategic Roadmap: Estonia.* Tallinn: Ministry of Economic Affairs and Communications. As of 27 March 2025: https://mkm.ee/sites/default/files/documents/2024-09/Estonian%20National%20Digital%20Decade%20Strategic%20Roadmap%202023.pdf#page=6.80

European Commission. n.d. 'Europe's Digital Decade: Digital Targets for 2030.' As of 9 April 2025: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

———. 2024a. *Estonia 2024 Digital Decade Country Report.* Brussels: European Commission. As of 9 April 2025: https://digital-strategy.ec.europa.eu/en/factpages/estonia-2024-digital-decade-country-report

———. 2024b. *Finland 2024 Digital Decade Country Report.* Brussels: European Commission. As of 27 March 2025: https://digital-strategy.ec.europa.eu/en/factpages/finland-2024-digital-decade-country-report

———. 2024c. *Poland 2024 Digital Decade Country Report.* Brussels: European Commission. As of 27 March 2025: https://digital-strategy.ec.europa.eu/en/factpages/poland-2024-digital-decade-country-report

———. 2024d. *Sweden 2024 Digital Decade Country Report.* Brussels: European Commission. As of 27 March 2025: https://digital-strategy.ec.europa.eu/en/factpages/sweden-2024-digital-decade-country-report

———. 2025a. 'The EU Cybersecurity Act.' As of 9 April 2025: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

———. 2025b. 'European Approach to Artificial Intelligence.' As of 9 April 2025: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

EIOPA (European Insurance and Occupational Pension Authority). n.d. 'Digital Operational Resilience Act (DORA).' As of 9 April 2025: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

EEAS (European External Action Service). 2017. 'EU and NATO Inaugurate European Centre of Excellence for Countering Hybrid Threats.' 2 October. As of 9 April 2025: https://www.eeas.europa.eu/node/33119_en

Federation of American Scientists. n.d. 'Section 2: Intelligence Collection Activities and Disciplines.' In *Operations Security: Intelligence Threat Handbook.* As of 29 March 2025: https://irp.fas.org/nsa/ioss/threat96/part02.htm#:~:text=Several%20intelligence%20disciplines%20are%20used,open%20source%20intelligence%20(OSINT)

Finnish Defence Forces. n.d. 'Digitalisaatio Puolustusvoimissa' [Digitalisation in the Defence Forces.] As of 27 March 2025: https://puolustusvoimat.fi/digitalisaatio

Finnish Government. 2021. *Government's Defence Report*. Helsinki: Finnish Government. As of 27 March 2025: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163407/VN_2021_80.pdf

———. 2024a. *Finland's National Roadmap: EU Digital Decade Policy Programme 2030.* Helsinki: Finnish Government. As of 27 March 2025: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165438/VN_2024_7.pdf?sequence=1&isAllowed=y

———. 2024b. 'Ministerial Working Group Updates the Measures of the Digital Compass that Guides Finland's Digital Transformation.' 17 December. As of 27 March 2025: https://valtioneuvosto.fi/en/-/1410829/ministerial-working-group-updates-the-measures-of-the-digital-compass-that-guides-finland-s-digital-transformation

Finnish Ministry of Defence. 2024. *Government Defence Report.* Helsinki: Finnish Government. As of 27 March 2025: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/166004/PLM_2024_7.pdf?sequence=4&isAllowed=y

Finnish Prime Minister's Office. 2024. *Finland's Cyber Security Strategy 2024-2035.* Helsinki: Prime Minister's Office. As of 27 March 2025: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf#page=12.21

Finlan, Alastair. 2024. 'A Fertile Soil for AI? Defense AI in Sweden.' In *The Very Long Game: 25 Case Studies on the Global State of Defense AI*, edited by Heiko Borchert, Torben Schütz & Joseph Verbovszky, 107-126. Cham: Springer. As of 27 March 2025: https://link.springer.com/chapter/10.1007/978-3-031-58649-1_5

French Institute for Higher National Defence Studies. n.d. 'Estonia: A digital Giant.' As of 27 March 2025: https://ihedn.fr/en/notre-selection/lestonie-un-geant-numerique/

Government Offices of Sweden. n.d.a. 'Total Defence'. As of 27 March 2025: https://www.government.se/government-policy/total-defence/

———. n.d.b. 'Defence Resolution 2025-2030'. As of 27 March 2025: https://www.government.se/government-policy/total-defence/defence-resolution-2025-20302/

Granlycke, Christer. 2024. 'Business Finland Launches Digital Resilience Program.' *Forum Nordic.* August 18. As of 27 March 2025: https://forumnordic.com/industry/business-finland-launches-digital-resilience-program/

Gubbels, Frank. 2023. 'NATO's Interoperability Challenge: Is FMN on Its Own?' *NATO Command and Control Centre of Excellence*. As of 9 April 2025: https://c2coe.org/wp-content/uploads/Library%20Documents/Annual%20Overviews/Articles/Annual%20Overview%202022/20230301%20Annual%20Overview%202022%20-%20NATOs%20Interoperability%20Challenge%20is%20FMN%20on%20its%20own.pdf#page=3.25

Hall, Jonny & Hugh Sandeman. 2022. *NATO's Resilience: The First and Last Line of Defence*. London: LSE Ideas. As of 27 March 2025: https://www.jstor.org/stable/pdf/resrep45244.pdf?refreqid=fastly-default%3A0634b2476911b573396841143c11c4bb&ab_segments=&initiator=&acceptTC=1#page=6.67

Ilves, Toomas. 2024. 'Digitizing Democracy: Former Estonian President on How e-Government Saved a Struggling Country.' *Vision*. March. As of 27 March 2025: https://vision.protiviti.com/insight/digitizing-democracy-former-estonian-president-how-e-government-saved-struggling-country

International Trade Administration. 2024c. 'Sweden – Digital Economy'. As of 27 March 2025: https://www.trade.gov/country-commercial-guides/sweden-digital-economy

———. 2024a. 'Poland ICT the Most Cyber Attacked Country in the World.' 28 February. As of 27 March 2025: https://www.trade.gov/market-intelligence/poland-ict-most-cyber-attacked-country-world

———. 2024b. 'Poland Cybersecurity and Digitization Strategy.' 30 October. As of 27 March 2025: https://www.trade.gov/market-intelligence/poland-cybersecurity-and-digitization-strategy

Internet Stiftelsen. n.d. 'Om Tänk säkert' [About Thinking Safe.] As of 4 April 2025: https://internetstiftelsen.se/tanksakert/om/

Jack, Victor. 2024. 'UK Warning: Russia's "Aggressive" Cyber Warfare Is Threat to NATO.' *Politico*, 24 November. As of 29 March 2025: https://www.politico.eu/article/russias-aggressive-cyberattack-putin-poses-threat-nato-uk/

Järvinen, Sami O. 2024. 'Cautious Data-Driven Evolution: Defence AI in Finland.' In *The Very Long Game: 25 Case Studies on the Global State of Defense AI*, edited by Heiko Borchert, Torben Schütz & Joseph Verbovszky, 127-148. Cham: Springer. As of 27 March 2025: https://link.springer.com/chapter/10.1007/978-3-031-58649-1_6

Jermalavičius, Tomas. 2024. 'Caught Between Today and Tomorrow: Defence AI in Estonia' In *The Very Long Game: 25 Case Studies on the Global State of Defense AI*, edited by Heiko Borchert, Torben Schütz & Joseph Verbovszky, 149-171. Cham: Springer. As of 27 March 2025: https://link.springer.com/chapter/10.1007/978-3-031-58649-1_7

Jones, Seth. 2025. 'Russia's Shadow War Against the West.' *Center for Strategic & International Studies*, 18 March. As of 29 March 2025: https://www.csis.org/analysis/russias-shadow-war-against-west

Kallenborn, Zachary. 2024. 'Swarm Clouds on the Horizon? Exploring the Future of Drone Swarm Proliferation.' *Modern War Institute at West Point*, 20 March. As of 29 March 2025: https://mwi.westpoint.edu/swarm-clouds-on-the-horizon-exploring-the-future-of-drone-swarm-proliferation/

Karjalainen, Anna-Maija. 2020. 'Digitalisation Is a Key Enabler for Public Sector Renewal.' *State Treasury Republic of Finland.* As of 27 March 2025: https://www.treasuryfinland.fi/annualreview2020/digitalisation-is-a-key-enabler-for-public-sector-renewal/

Kaska, Kadri, Anna-Maria Osula, LTC Jan Stinissen 2013. *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. As of 27 March 2025: https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf#page=7.12

Kattel, Rainer & Ines Mergel. 2019. 'Estonia's Digital Transformation: Mission Mystique and the Hiding Hand.' In *Great Policy Successes*, edited by Paul Hart & Mallory Compton, 143-160. Oxford: Oxford University Press. As of 27 March 2025: https://academic.oup.com/book/42635/chapter/358101931

Khorrami, Nima. 2024. 'Sweden's Defense Overhaul: Prioritizing NATO, Baltic Security, and Space Capabilities.' *Wilson Center.* 23 October. As of 27 March 2025: https://www.wilsoncenter.org/article/swedens-defense-overhaul-prioritizing-nato-baltic-security-and-space-capabilities

Krasavina, Andra. 2024. 'Sweden – National Digital Decade Strategic Roadmap.' *EU Digital Skills & Jobs Platform.* 5 August. As of 27 March 2025: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/sweden-national-digital-decade-strategic-roadmap

Lindfors, Jonny, Jan Lundberg & Filip Scheynius. 2024. 'Preparing for the Next War: An Analysis of the Swedish Army's Needs for Transformation.' *The Royal Swedish Academy of War Sciences.* 15 October. As of 27 March 2025: https://kkrva.se/preparing-for-the-next-war-an-analysis-of-the-swedish-armys-needs-for-transformation/

Lucarelli, Sonia, Alessandro Marrone & Francesco N. Moro. 2021. *NATO Decision-Making in the Age of Big Data and Artificial Intelligence.* Brussels: NATO Headquarters. As of 27 March 2025: https://www.act.nato.int/wp-content/uploads/2024/07/20210301_AC-2020_Final-Report.pdf

Lucas, Rebecca, Stella Harrison, Conlan Ellis, James Black, Ben Fawkes, Martin Robson, Alan Brown & Edward Keedwell. 2024. *Command and Control in the Future: Concept Paper 4 – C2 Enablers*. Santa Monica, Calif.: RAND Corporation. RR-A2476-4. As of 29 March 2025: https://www.rand.org/pubs/research_reports/RRA2476-4.html

Melhem, Samia & Astrid Herdis Jacobsen. 2021. 'A Global Study on Digital Capabilities'. World Bank Group. As of 28 March 2025: https://documents1.worldbank.org/curated/en/959181623060169420/pdf/A-Global-Study-on-Digital-Capabilities.pdf#page=10.09

NATO (North Atlantic Treaty Organisation). 2009. 'The North Atlantic Treaty (1949).' As of 9 April 2025: https://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf

———. 2016. 'Warsaw Summit Communiqué.' 9 July. As of 9 April 2025: https://www.nato.int/cps/cn/natohq/official_texts_133169.htm

———. 2021a. 'Brussels Summit Communiqué.' Press release. 14 June. As of 29 March 2025: https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en

———. 2021b. 'NATO 2030.' Factsheet. June. As of 29 March 2025: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf

———. 2021c. 'Strengthened Resilience Commitment.' 14 June; last updated 13 September 2022. As of 9 April 2025: https://www.nato.int/cps/en/natohq/official_texts_185340.htm

———. 2022c. 'Madrid Summit Declaration.' 29 June. As of 29 March 2025: https://www.nato.int/cps/cn/natohq/official_texts_196951.htm

———. 2022a. 'NATO Strategic Concept.' 29 June. As of 29 March 2025: https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf

———. 2022b. 'NATO Defence Planning Process.' 31 March. As of 9 April 2025: https://www.nato.int/cps/en/natohq/topics_49202.htm

———. 2022d. 'Resilience Committee.' 7 October. As of 9 April 2025: https://www.nato.int/cps/in/natohq/topics_50093.htm

———. 2022e. 'NATO's Nuclear Sharing Arrangements.' Factsheet. February. As of 9 April 2025: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/2/pdf/220204-factsheet-nuclear-sharing-arrange.pdf

———. 2022f. 'Standardization.' 14 October. As of 9 April 2025: https://www.nato.int/cps/cn/natohq/topics_69269.htm

———. 2023b. 'Interoperability: Connecting Forces.' 11 April. As of 29 March 2025: https://www.nato.int/cps/fr/natohq/topics_84112.htm?selectedLocale=en

———. 2023a. 'Vilnius Summit Communiqué.' Press release. 11 July. As of 29 March 2025: https://www.nato.int/cps/ge/natohq/official_texts_217320.htm

———. 2024a. 'NATO Allies Take Stock of Progress on Digital Initiatives.' 18 November. As of 29 March 2025: https://www.nato.int/cps/en/natohq/news_230435.htm

———. 2024g. *NATO Digital Backbone and NATO Digital Backbone Reference Architecture.* NATO. As of 29 March 2025: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/12/pdf/241213-DBRA.pdf

———. 2024d. 'NATO Steps Up Alliance-Wide Secure Data Sharing.' 17 October. As of 29 March 2025: https://www.nato.int/cps/fr/natohq/news_229523.htm?selectedLocale=en

———. 2024c. 'NATO's Strategy for Digital Transformation'. 22 October. As of 28 March 2025: https://www.nato.int/cps/en/natohq/news_229985.htm

———. 2024e. 'Washington Summit Declaration.' Press release. 10 July. As of 29 March 2025: https://www.nato.int/cps/cn/natohq/official_texts_227678.htm

———. 2024a. *NATO Standard: AJP-6: Allied Joint Doctrine for Communication and Information Systems: Edition B, Version 1.* NATO Standardization Office. As of 9 April 2025: https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDB_V1_E_2525.pdf

———. 2024b. 'Digital Policy Committee (DPC)'. 31 January. As of 9 April 2025: https://www.nato.int/cps/ua/natohq/topics_69279.htm

———. 2024e. 'Allied Command Operations (ACO).' 27 May. As of 9 April 2025: https://www.nato.int/cps/eu/natohq/topics_52091.htm

———. 2024f. 'Emerging and Disruptive Technologies.' 8 August. As of 9 April 2025: https://www.nato.int/cps/bu/natohq/topics_184303.htm#ip4

———. 2024h. 'Resilience, Civil Preparedness and Article 3.' 13 November. As of 9 April 2025: https://www.nato.int/cps/uk/natohq/topics_132722.htm?selectedLocale=en

———. 2025. 'NATO's Digital Transformation Implementation Strategy.' NATO Press Office, 20 February. As of 28 March 2025: https://www.nato.int/cps/en/natohq/official_texts_229801.htm

NATO ACT (Allied Command Transformation). n.d.a. 'Federated Mission Networking.' As of 9 April 2025: https://www.act.nato.int/activities/federated-mission-networking/

———. n.d.b. 'Centres of Excellence.' As of 9 April 2025: https://www.act.nato.int/about/centres-of-excellence/

———. 2022. 'Multi-Domain Operations: Enabling NATO to Out-Pace and Out-Think Its Adversaries.' 29 July. As of 29 March 2025: https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/#:~:text=The%20NATO%20'working'%20definition%20of,at%20the%20speed%20of%20relevance%E2%80%9D

———. 2023a. 'Empowering NATO's Multi-Domain Operations Through Digital Transformation.' 16 October. As of 29 March 2025: https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/

———. 2023b. 'Multi-Domain Operations in NATO – Explained.' 5 October. As of 29 March 2025: https://www.act.nato.int/article/mdo-in-nato-explained/

———. 2023a. *Allied Command Transformation: 20 Years as NATO's Military Leader for Change*. NATO Allied Command Transformation. As of 9 April 2025: https://www.act.nato.int/wp-content/uploads/2023/06/NATO-booklet-2023-LR.pdf

———. 2024. 'NATO Centres of Excellence: Powering the Alliance's Digital Transformation'. 2 April. As of 28 March 2025: https://www.act.nato.int/article/coes-powering-alliance-digital-transformation/

NATO C2COE (Command and Control Centre of Excellence). 2020. 'Federated Mission Networking (FMN).' *NATO C2COE Expertise Management Branch*. As of 9 April 2025: https://c2coe.org/wp-content/uploads/Library%20Documents/QRL/2020/QRL_C2COE%202020%20Federated%20Mission%20Networking%20%28FMN%29.pdf

———. n.d.a. 'Service Portfolio.' As of 9 April 2025: https://www.ncia.nato.int/about-us/service-portfolio

NATO Modelling & Simulation Group. n.d. 'NATO M&S.' As of 9 April 2025: https://nmsg.sto.nato.int/

NATO Strategic Communications Centre of Excellence. 2020. *Clarifying Digital Terms*. NATO Strategic Communications Centre of Excellence. As of 28 March 2025: https://stratcomcoe.org/cuploads/pfiles/digital_terminology_nato_stratcom_coe_14-10-2020.pdf

NCSC (National Cyber Security Centre). 2022. 'Russia Behind Cyber Attack with Europe-Wide Impact an Hour Before Ukraine Invasion.' 10 May. As of 29 March 2025: https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion

NCI (NATO Communications and Information) Agency. n.d.b. 'Technology and Innovation.' As of 9 April 2025: https://www.ncia.nato.int/about-us/technology-and-innovation

NIFC (NATO Intelligence Fusion Centre). n.d. 'Who We Are.' As of 9 April 2025: https://web.ifc.bices.org/about-us/who-we-are

Northrop Grumman. 2024. 'Integrated Battle Command System Achieves Initial Operational Capability in Poland.' News release. 19 December. As of 27 March 2025: https://news.northropgrumman.com/news/releases/integrated-battle-command-system-achieves-initial-operational-capability-in-poland

O'Dwyer, Gerard. 2023. 'Swedish Government Launches Accelerated Digitisation Plan.' *ComputerWeekly.com*, 19 January. As of 27 March 2025: https://www.computerweekly.com/news/252529304/Swedish-government-launches-accelerated-digitisation-plan

Office for Budget Responsibility. 2022. 'Cyber-Attacks During the Russian Invasion of Ukraine.' July. As of 28 March 2025: https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/

Petersen, Michael. 2016. 'The Perils of Conventional Deterrence by Punishment.' *War on the Rocks*, 11 November. As of 29 March 2025: https://warontherocks.com/2016/11/the-perils-of-conventional-deterrence-by-punishment/

Polish Ministry of Digital Affairs. 2024. 'Strategia Cyfryzacji Polski do 2035 roku' [Digitalisation Strategy of Poland until 2035]. 29 October. As of 27 March 2025: https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-polski-do-2035-roku

———. 2025. 'Warsaw Call on Cybersecurity Challenges.' As of 27 March 2025: https://polish-presidency.consilium.europa.eu/media/bkmbggs0/warsaw-call_en.pdf

Polish Ministry of National Defence. 2024. 'Resortowa strategia sztucznej inteligencji do roku 2039' [Ministry's Artificial Intelligence Strategy Until 2039]. 11 October. As of 27 March 2025: https://www.gov.pl/web/obrona-narodowa/resortowa-strategia-sztucznej-inteligencji-do-roku-2039

Polish Presidency Council of the European Union. 2025. 'Warsaw Call Declaration Adopted at the Informal TTE Telecom Council on Cybersecurity.' Press release. 5 March. As of 27 March 2025: https://polish-presidency.consilium.europa.eu/en/news/warsaw-call-declaration-adopted-at-the-informal-tte-telecom-council-on-cybersecurity/

Ptak, Alicja. 2024. 'Poland Records Europe's Second-Largest Improvement in Digital Public Services.' *Notes from Poland.* 5 July. As of 27 March 2025: https://notesfrompoland.com/2024/07/05/poland-records-europes-second-largest-improvement-in-digital-public-services/

Reuters. 2024. 'Poland to Boost Cybersecurity After Fake News Attack.' 3 June. As of 27 March 2025: https://www.reuters.com/technology/cybersecurity/poland-spend-3-bln-zlotys-cybersecurity-after-attack-news-agency-2024-06-03/

Rodriguez, Cesar Augusto, Timothy Charles Walton & Hyong Chu. 2020. 'Putting the "FIL" in "DIME": Growing Joint Understanding of the Instruments of Power.' *Joint Force Quarterly* 97, 1 April. As of 29 March 2025: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106566/putting-the-fil-into-dime-growing-joint-understanding-of-the-instruments-of-pow/

Roepke, Wolf-Diether & Hasit Thankey. 2019. 'Resilience: The First Line of Defence.' *NATO Review*, 27 February. As of 27 March 2025: https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html

Ruth, Oliver. 2025. 'The Impact of Sanctions and Alliances on Russian Military Capabilities.' *Royal United Services Institute,* 10 January. As of 29 March 2025: https://www.rusi.org/explore-our-research/publications/commentary/impact-sanctions-and-alliances-russian-military-capabilities

Saab. 2024. 'Saab in New Partnership with FMV Digitalizing the Ground Forces of the Swedish Armed Forces (FM).' 11 September. As of 27 March 2025: https://www.saab.com/newsroom/stories/2024/september/saab-in-new-partnership-with-fmv-digitalizing-the-ground-forces-of-the-swedish-armed-forces-fm

Schneider. 2025. *Digitally-Enabled Warfare: The Capability-Vulnerability Paradox*. Washington: Centre for a New American Security. As of 28 March 2025: https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox

Shea, Jamie. 2025. 'Space and Cyberspace: NATO's New Frontier of Defence.' *Defence Studies*, 26 March. As of 9 April 2025: https://www.tandfonline.com/doi/pdf/10.1080/14702436.2025.2474069

Soare, Simona R. 2023. *Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age*. London: The International Institute for Strategic Studies. As of 27 March 2025: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/08/digitalisation-of-defence-in-nato-and-the-eu-making-european-defence-fit-for-the-digital-age.pdf#page=6.05

Spirtas, Michael. 2018. 'Toward One Understanding of Multiple Domains.' *RAND Corporation*. 2 May. As of 9 April 2025: https://www.rand.org/pubs/commentary/2018/05/toward-one-understanding-of-multiple-domains.html

Supreme Headquarters Allied Power Europe NATO. n.d. 'Operations.' As of 9 April 2025: https://shape.nato.int/operations

Swedish Ministry of Defence. 2024. *Strategic Direction for Defence Innovation*. Stockholm: Ministry of Defence. As of 27 March 2025: https://www.government.se/contentassets/f095f1d430164d2c9af6d66a40a30130/strategic-direction-for-defence-innovation.pdf#page=4.05

Swedish Ministry of Foreign Affairs. 2024. *Sweden in a Digital World: A Strategy for Sweden's Foreign And Security Policy on Cyber and Digital Issues*. Stockholm: Ministry of Foreign Affairs. As of 27 March 2025: https://www.government.se/contentassets/f858cec8cb944d3fa82bdf0fb7959448/sweden-in-a-digital-world---a-strategy-for-swedens-foreign-and-security-policy-on-cyber-and-digital-issues.pdf

Swicord, Ellen. 2022. 'NATO's New Strategic Concept: What It Is and Why It Matters'. *Nuclear Threat Initiative*, 20 July. As of 29 March 2025: https://www.nti.org/risky-business/natos-new-strategic-concept-what-it-is-and-why-it-matters/

Szeleczki, Szilveszter. 2019. 'Interpreting the Interoperability of the NATO's Communication and Information Systems.' *Scientific Bulletin* 24 (1): 95-107. As of 27 March 2025: https://intapi.sciendo.com/pdf/10.2478/bsaft-2019-0011#page=12.25

The Baltic Times. 2025. 'Number of Impactful Cyber Incidents in Estonia Nearly Doubled on Year.' 4 February. As of 9 April 2025: https://www.baltictimes.com/number_of_impactful_cyber_incidents_in_estonia_nearly_doubled_on_year/

Tillberg, Lotta V., Joakim Berndtsson & Peter Tillberg. 2025. 'Navigating Collaboration: Understanding Civil-Military Interactions in Swedish Total Defence from a Security Network Perspective.' *Scandinavian Journal of Military Studies* 8 (1): 40-56. As of 27 March 2025: https://sjms.nu/articles/288/files/67938188cb01f.pdf#page=2.05

U.S. Department of Defense. 2022. 'DoD Announces Release of JADC2 Implementation Plan.' 17 March. As of 29 March 2025: https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/

Vinnova. 2024. 'Vinnova: Civil Innovations Will Strengthen Sweden's Defense Capabilities.' *Science Business,* 24 June. As of 27 March 2025: https://sciencebusiness.net/network-updates/vinnova-civil-innovations-will-strengthen-swedens-defense-capabilities

Welch, Carley. 2024. 'NATO Agency Unveils First-of-its-Kind Tech Strategy for Multi-Domain Operations.' *Breaking Defense,* 4 December. As of 27 March 2025: https://breakingdefense.com/2024/12/nato-agency-unveils-first-of-its-kind-tech-strategy-for-multi-domain-operations/

Yasar, Kinza. 2023. 'Definition: Digital.' *TechTarget*, November. As of 9 April 2025: https://www.techtarget.com/whatis/definition/digital

List of figures, tables & boxes

Abbreviations and acronyms

5G	fifth-generation (telecommunications technology)
6G	sixth-generation (telecommunications technology)
ACO	Allied Command Operations (NATO)
ACT	Allied Command Transformation (NATO)
ADSE	Alliance Data Sharing Ecosystem (NATO)
AI	artificial intelligence
C2	command and control
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
CCDCOE	Cooperative Cyber Defence Centre of Excellence (NATO)
CIS	communications and information systems
COE	centre(s) of excellence
DIANA	Defence Innovation Accelerator for the North Atlantic (NATO)
DIME-FIL	diplomatic, information, military, economic, finance, intelligence and law enforcement
DDA	Deterrence and Defence of the Euro-Atlantic Area (NATO)
DPC	Digital Policy Committee (NATO)
DOTMLPFI	doctrine, organization, training, materiel, leadership development, personnel, facilities and interoperability
e-ID	electronic identification
EC	European Commission (EU)
EU	European Union
FMN	federated mission networking
GDP	gross domestic product
IBCS	Integrated Battle Command System
ICT	information and communications technology
ISR	intelligence, surveillance and reconnaissance
IT	information technology

LOE	line(s) of effort
MDO	multi-domain operations
ML	machine learning
NASA	National Aeronautics and Space Administration (United States)
NATO	North Atlantic Treaty Organization
NCI Agency	NATO Communications and Information Agency
NDBB	NATO Digital Backbone
NDDP	NATO Defence Planning Process
OODA	observe-orient-decide-act
OSCE	Organization for Security and Co-operation in Europe
R&D	research and development
SAF	Swedish Armed Forces
SHAPE	Supreme Headquarters Allied Powers Europe (NATO)
UK	United Kingdom

Acknowledgements

The authors are grateful to Microsoft for their sponsorship of this study and their support throughout the research. In particular, thanks are owed to Simon van Hoeve and Ben Crampton.

In addition, the team would like to thank all those who agreed to participate in interviews, as their insights and impressions were critical in ensuring that we incorporated a variety of perspectives. As agreed, all contributions have been anonymised.

Finally, the team are thankful for the comments and advice provided by RAND quality assurance reviewers James Black and Lucia Retter.

Despite these valued contributions, any errors or omissions remain the sole responsibility of the authors.