DIGITAL SHIELD: INTEGRATING HEALTH INTELLIGENCE INTO NATO'S DEFENSE STRATEGY

Dimitra BALASKA*, Dimitris KARAFERIS*,

Ioannis REMATISIOS*, Yannis POLLALIS*

*Department of Economic Science-iLEADS Lab,
University of Piraeus, Piraeus, Greece

The COVID-19 pandemic and Russia's war against Ukraine have reshaped how security is perceived, exposing the interdependence of health, defence and digital infrastructures. National security must therefore broaden to include health resilience as a core operational priority. As NATO and the EU move forward with digital transformation, embedding health intelligence becomes essential for readiness, force protection and civil–military cooperation. This paper argues that real-time health data, wearable devices and AI-enabled surveillance can support not only responses to biological threats but also anticipation of vulnerabilities before they escalate. By shifting from reactive to proactive postures, NATO and the EU can build more resilient and human-centred security frameworks adapted to hybrid warfare. Recognising health systems as critical infrastructure, alongside energy and transport, makes integration a strategic necessity. Doing so will shape the credibility, adaptability and resilience of NATO and the EU in decades ahead, strengthening security in an increasingly complex environment.

Key words: *health intelligence integration, hybrid security threats, biosecurity, health & safety, quality in health care.*

1. INTRODUCTION

The COVID-19 pandemic and the war in Ukraine have revealed something very important: health is no longer distinct from security and defense. When issues of national sovereignty or biological threats arise, defense is immediately affected. These new realities drive NATO and the EU to quickly embrace the idea of digital transformation. Digital transformation in defense is not just about using better technology. It is about creating smarter, faster, and more integrated systems that help both military and

civilian organizations make better decisions. This includes using real-time data, artificial intelligence, and secure communication platforms that can support everything from military operations to public health emergencies (Anghel and Jones, 2023; Fiott, 2023; Csernatoni and Martins, 2024).

While the term "digital transformation" used broadly, its true meaning goes beyond just adopting new technologies or digitizing old processes. Digitization, converting analog data into digital format, is just the first step. True digital transformation involves redesigning how organizations work, how decisions are made, and how people interact with systems. It is not just about emails, dashboards, modernization or AI deployment. Instead, digital transformation is about building secure, flexible, and interconnected systems that bring together real-time data from various sources. These systems help make faster, better decisions by integrating everything from cloud infrastructure and APIs to AI, sensors, and next-gen communications. For NATO and the EU, this means rethinking how data managed across defense forces, from logistics to battlefield intelligence to health monitoring, and turning it into a strategic asset. Ultimately, digital transformation is about making defense smarter, faster and more responsive, not just through technology but through cultural, organizational, and procedural change. It is a journey toward an adaptive, data-driven defense model that supports both operational effectiveness and the well-being of personnel. Nevertheless, NATO pursues three additional core tasks in addition to collective defense, namely crisis prevention, management and cooperative security. It may encompass both military and non-military strategies to tackle the entire range of crises—prior to, during, and following conflicts, as well as in reaction to natural disasters, acts of terrorism, technological disturbances, public health crises, or any other situation that could jeopardize the security of Allied nations (Burwell, 2020; Ilangakoon et al., 2022; Mauro et al., 2024).

National initiatives to prioritize the digital transformation of defense and ongoing efforts within NATO and the EU are a step in the right direction. However, the current conception and planning of defense digitalization within national capitals and the two organizations – NATO and the EU – is insufficiently understood, overly incremental, and lacks the necessary scope to transform European defense at a pace that is relevant. Despite the policy narrative acknowledging "the urgency of a digitally-transformed Alliance," NATO's development of its digital transformation agenda has been years in the making.

Furthermore, its implementation process, linked to capability development, is a decades-long effort where 2030 (for NATO, even later for individual allies) is merely the first milestone for basic capability levels. Both NATO and the EU seem to have resigned themselves to a "fast-follower" approach to digitalization, where neither states nor the EU or NATO are leading the way in the digital transformation of defense, but instead responding to much larger structural shifts in the digital revolution within industry. Europe's efforts to transform its defense and become a competitive and credible defense actor are not progressing fast enough. Its poor track record on defense digitalization over the past few decades suggests that its defense leadership has not fully embraced the challenge. Europe has persisted with an approach to digital transformation which characterized by incrementalism and selective implementation. It has done so even in the face of strategic threats to European defense, most notably the aggression from Russia in its war against Ukraine, demonstrating a degree of strategic paralysis in Europe. These challenges are not only affecting military readiness but also the overall health of European defense systems, including the ability to adapt to technological advancements and address critical security and health-related issues that arise in the digital age (Gilli, 2020; Fasola, 2024; NATO's strategy for digital transformation, 2024).

In recent years, NATO and the EU have both adopted ambitious digital strategies. But while the focus is often on weapons systems or cyber security, there is growing recognition that health intelligence must be part of this transformation. Health data, collected through wearables, field diagnostics, and surveillance systems, can help anticipate crises, protect personnel, and support civil-military cooperation in times of need. Health is becoming an operational concern. Beyond its role in crisis response, robust health data enables better planning, enhances troop readiness, and strengthens supply chains. The ability to predict and respond to biological risks, mental health strain, or logistical gaps in medical support can dramatically impact operational outcomes. As NATO and the EU move forward with their digital ambitions, integrating health intelligence will be essential for creating a comprehensive, human-centered security strategy (Bricknell M. *et al.*, 2020; Mesterhazy, 2020; Policy Department, 2021).

As The COVID-19 pandemic has highlighted the significance of biological agents as a distinct threat vector that poses a risk to the security of NATO member states. This study examines the potential for a more profound integration of health intelli-

gence within NATO's digital defense strategy, particularly in relation to the requirements for medical military support. By doing so, we contend that NATO has the potential to develop a more robust, agile, and adaptable strategy for contemporary security, wherein digital technologies not only improve military effectiveness but also collective security safeguard the health and welfare of service members and the civilians they are committed to protecting.

2. DEFINING HEALTH INTELLIGENCE AND INTEGRATION CRITERIA

Health intelligence (HI) is widely understood as the systematic collection, analysis and interpretation of data about health, health systems, health threats and the wider determinants of health for the purposes of decision-making and resource allocation. The World Health Organization (WHO) notes that health intelligence involves the systematic collection and analysis of data on health, health systems, health threats and wider determinants of health, while the Pan American Health Organization defines it as the analysis of population health, health system performance and health research (Haby *et al.*, 2023). In military contexts, medical intelligence is defined as the collection, evaluation and analysis of foreign medical, bio-scientific and environmental information that informs strategic planning and medical operations (Bowsher, Milner and Sullivan, 2016). In this paper, the term health intelligence encompasses both public health intelligence and military medical intelligence; it refers to the capability to gather and synthesize timely health-related information in order to protect personnel, anticipate threats and inform operational planning.

To evaluate the successful integration of health intelligence across defense, healthcare and civil-military organizations, we propose several indicative criteria. First, organizations must be able to capture and share multi-sectoral data, including private-sector metrics and subnational capacities, in near real time. Second, the availability and capacity for electronic surveillance and high-quality data must be assessed, including timeliness of routine reporting and data quality scores. Third, integration readiness can be measured by the existence of digital infrastructures and trained personnel capable of collecting, analyzing and disseminating health intelligence across agencies. Fourth, tracking indicators such as internally displaced persons, returnees and other vulnerable groups improves preparedness, as emphasized by public health experts (Erondu *et al.*, 2021). Together these criteria provide a starting point for evaluating the maturity of health intelligence integration.

3. NATO'S DIGITALIZATION OF DEFENSE: PROGRESS AND CHALLENGES

Digitalization in defense is steadily gaining momentum within NATO. In October 2022, Alliance leaders officially endorsed a vision for digital transformation and approved the NATO Data Exploitation Framework Policy (DEFP). This was followed in July 2023 by the adoption of the Digital Transformation Implementation Strategy, which aligns digital transformation milestones with NATO's capability development objectives and interoperability standards. NATO views digital transformation as a fundamental enabler and driver of seamless integration across domains, facilitating Multi-Domain Operations (MDO). As noted by NATO's Digital Transformation Champion and Special Advisor Didier Polomé, the goal is that by 2030, NATO's digital transition will empower the Alliance to execute MDO, ensure interoperability across all operational areas, enhance situational awareness, and support both political consultations and data-driven decision-making. This strategy is rooted in NATO's operational requirements outlined in a range of strategic documents, such as the 2019 Military Strategy, the Warfighting Capstone Concept, the evolving MDO concept, the AI Strategy, and the DEFP. These documents collectively set the path for NATO's shift toward multi-domain operational capabilities by 2030. Beyond the military dimension, digital transformation is intended to be fully integrated with NATO's Defence Planning Process, capability development targets, standardization efforts, R&D, procurement processes, and high-tech initiatives like DIANA (Defence Innovation Accelerator for the North Atlantic) (NATO, 2021, 2023b, 2023a, NATO STO SET Panel, 2022; Soare, 2023).

As shown in the associated Figure 1, the transformation rests on five core components and three structural pillars. Key technologies include cloud computing, a modular open-system digital infrastructure, a federated synthetic environment, and a smart data fabric that facilitates the processing and sharing of data across platforms and users. Cybersecurity addressed through a "zero trust" approach. However, the greatest challenge may lie not in technology, but in fostering a culture that promotes innovation, experimentation, information sharing, and responsible risk-taking by both American and European companies. This requires a culture change from leaders/governments and decision makers, as they are usually not willing to accept early failures in collaborative R&D initiatives to stay ahead of the innovation curve against their competitors. The return on investment (ROI) for defense technologies at initial TRL levels is

mostly intangible, while Member States usually aim for tangible results (through industrial benefits). This shift also demands a digitally literate workforce, and NATO estimates that by 2030, at least 10% of its personnel must have digital competencies, representing a fivefold increase from current figures (NATO STO SET Panel, 2022; Soare, 2023; Shaun Cannon, 2024, NATO Reflection Group, 2020; Rauch et al., 2024).

While the scale of NATO's digital strategy is ambitious, concerns persist around the complexity of its implementation and the internal division of responsibilities. Operational leadership lies with Allied Command Transformation and Allied Command Operations, while agencies like the NATO Communications and Information Agency, NATO Support and Procurement Agency, and the Alliance CIO provide support. Political and policy coordination is driven by NATO's International Staff, including the CIO, the Emerging Security Challenges Division, and the Consultation, Command and Control Board. Despite this structure, internal collaboration has occasionally faltered, creating additional hurdles. Furthermore, digital transformation is seen as a continuous modernization process, with 2030 serving as a major milestone. However, the pace of progress remains a concern. Developing digital capabilities in Europe typically takes two to three years for concept development, with procurement often doubling or

Fig. 1 Pillars and building blocks of NATO's Digital Transformation to enable multi-domain operations (Soare, 2023)

tripling that timeline. Full delivery of digital solutions can require an additional three to four years, if not longer. Consequently, a comprehensive digitalization effort in European defense may span over a decade (Haddud and McAllen, 2018; Oberländer, Beinicke and Bipp, 2020; Fiott, 2023, Wolff, 2025).

Consequently, without urgent reforms to streamline procurement, align budgets and defense planning, and dramatically boost digital expertise within both NATO and national defense sectors, achieving the Alliance's 2030 digitalization goals remains unlikely. While incremental improvements may be achieved, the European pillar of NATO is expected to face significant difficulty meeting its digital transformation targets on time (Soare, 2023; Cannon S, 2024; NATO, 2024; NATO Reflection Group, 2020; Fiott, 2023a; Rauch et al., 2024; Haddud and McAllen, 2018; Oberländer, Beinicke and Bipp, 2020; Caliskan and Liégeois, 2021; Wolff, 2025).

4. BUILDING TECHNOLOGICAL SOVEREIGNTY THROUGH HEALTH: EU PROGRESS, CHALLENGES, AND NATO CONVERGENCE

The European Union has made notable progress in enhancing its strategic and technological sovereignty, particularly in the areas of health and security. Since 2019, the European Commission, in collaboration with Member States, has been shaping a robust agenda for the digital transformation of health systems across Europe (Burwell, 2022; Lantzsch *et al.*, 2022; Bocean and Vărzaru, 2025). The emphasis on technological and digital sovereignty, which are essential elements of the EU's strategic autonomy as digitalization gains significance for geopolitical influence and economic objectives, has intensified under the von der Leyen Commission. This focus has emerged in response to the rising significance of the data economy, escalating worries regarding the dominance and power centralization among a limited number of non-EU technology firms, and the potential reliance on external technologies, vital infrastructure, digital services, and the management and safeguarding of data from foreign entities. Key EU bodies, such as the Directorate-General for Health and Food Safety (DG SANTE), the Directorate-General for Communications Networks, Content and Technology (DG CONNECT), and the European Health and Digital Executive Agency (HaDEA), play a central role in advancing various facets of digital health. Their efforts supported through multiple EU-level funding mechanisms, including (Burwell, 2022; Lantzsch et al., 2022; Bocean and Vărzaru, 2025; Odone et al., 2019; Fahy N, 2021; Orăștean,

Sava and Mărginean, 2022; Crespi *et al.*, 2021; Ruohonen and Timmers, 2025; Madiega, 2020; Gallo et al., 2021; Baroncelli, 2024):

- *EU4Health Programme:* With a €5.3 billion budget for 2021–2027, this programme aims to strengthen health systems and foster digital health transfo-rmation.
- *Digital Europe Programme:* Supports projects in AI, cyber-security, and digital innovation across the EU.
- *Horizon Europe:* The EU's key research and innovation programme, which includes health-related actions to improve citizens' well-being and care.
- *Recovery and Resilience Facility (RRF):* Part of the NextGenerationEU plan, financing reforms and investments including those in digital health.
- *European Regional Development Fund (ERDF):* Supports infrastructure and service investments, including digital health initiatives, to promote economic and social cohesion.

In 2019, Finland and Estonia took the lead in advancing digital health integration within the EU, becoming the first member states to enable cross-border electronic prescriptions and patient data exchange. During Finland's Presidency of the Council of the European Union that same year, the strategic agenda placed strong emphasis on the digitalization of healthcare systems and the adoption of artificial intelligence (AI) to modernize health services. The focus was on creating interoperable digital infrastructures and fostering public-private partnerships to support innovation, enhance citizen wellbeing, and build resilience in European health systems. These early initiatives laid the groundwork for broader EU-level discussions on the integration of emerging technologies, such as AI, into healthcare frameworks and policy planning (Niño Sevilla Palma, 2021; Bocean and Vărzaru, 2025).

Despite progress, significant challenges remain. The European Court of Auditors has noted the complexity in tracking digital health funding and highlighted bureaucratic obstacles that limit the effective access to funds by some Member States. Moreover, while initiatives such as the EHDS promote interoperability and data sharing, critical gaps persist in areas such as cryptography, cloud infrastructure, and next-generation communi-cations. The **EU Strategic Compass** has reaffirmed the importance of investing in digital and emerging technologies as one of the Union's four strategic priorities in health. NATO has also expressed increasing interest in the convergence

of health and digital defense capabilities, particularly considering evolving hybrid threats. However, the EU's investment in digital health transformation currently surpasses NATO's in scope and funding. The management and funding of such new initiatives within NATO are primarily overseen and financed by DIANA and NIF, in close collaboration with the well-established SPS programme. This enhances the partnership between civilian science and technology (S&T) and creates extensive synergies involving NATO OCIO, NCIA, STO panels, academic institutions, and National Research Centers. The focus is on specific areas such as cyber, artificial intelligence, health, climate, and energy, which operate at various classification levels. There is a clear plan aimed at achieving tangible outcomes that lead to innovative solutions, which can be measured and justified to the member nations. DIANA serves as the innovation accelerator, linking innovators globally and utilizing test centers and accelerator sites to create solutions that meet NATO's operational needs, including health intelligence. Meanwhile, the NATO Innovation Fund (NIF) represents the first multi-sovereign venture capital fund dedicated to fostering the develop-pment of dual-use technologies that benefit both civilian and military sectors. Yet, implementation within the EU remains slower and more fragmented. The prioritization of the EU Rapid Deployment Capacity (RDC) further suggests that digital health efforts are still narrowly aligned with specific operational needs, rather than system-wide transformation (Bente *et al.*, 2024; Gaeta *et al.*, 2025).

While the EU has established strong institutional frameworks and funding tools for advancing digital health, coordinated and intensified efforts needed to overcome persistent gaps and ensure the effective implementation of digital health strategies across all Member States. Enhanced civil-military collaboration, including shared lessons with NATO, will be essential to building resilient and technologically sovereign health systems for the future (Bachmann, 2011; Fahy N, 2021).

NATO's Digital Transformation Implementation Strategy emphasizes multi-domain operations, alliance-wide interoperability and data-driven decision-making (NATO, 2023b). It focuses on building a digital backbone, data-sharing ecosystems, synthetic environments and a digitally ready workforce. By contrast, the EU's digital health agenda seeks to achieve technological and data sovereignty, investing heavily in public-sector infrastructure through programmes such as EU4Health, the Digital Europe Programme and the Recovery and Resilience Facility

(Sylvia N., 2025). The EU prioritizes cross-border e-health services, interoperable standards and national digital health ecosystems. These approaches are complementary. NATO's emphasis on operational interoperability and defense planning can benefit from the EU's investments in civilian health infrastructure, while EU initiatives on digital sovereignty and health data spaces can feed into NATO's data exploitation frameworks. Recognizing these synergies can help avoid duplication, align priorities and enhance collective security.

An instructive example of successful integration can be found in Estonia. The country has built a nationwide digital health information system that securely connects hospitals, clinics, pharmacies and citizens through the X-Road data-exchange platform. As a result, 99 % of patients in Estonia have digital health records and 100 % of prescriptions are issued electronically; the e-Health portal supports millions of queries each year (Enterprise Estonia, 2025). Estonia's Health Information System (EHIS) integrates data from birth to death and provides clear governance, legal clarity and agreed access rights for different actors (J.Metsallik *et al.*, 2018). This integrated infrastructure enables near-real-time health monitoring and improves decision-making for both civilian and military planners.

Nevertheless, it exposes important privacy and ethical considerations. Implementing AI-enabled health surveillance requires robust data

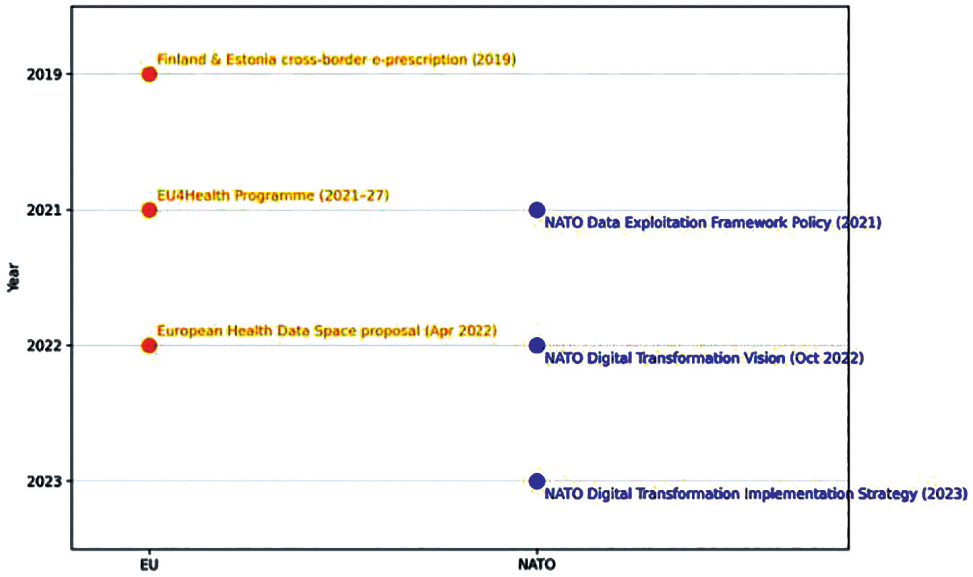

Fig. 2 Chronological milestones of NATO and EU digital transformation and health integration

protection, informed consent, algorithmic fairness, transparency and clear regulatory oversight to ensure public trust (Gerke, Minssen and Cohen, 2020). Estonia's experience also illustrates procurement challenges: replacing legacy systems requires long-term investment and flexible procurement models that prioritize interoperability and open standards. Roles and responsibilities are shared among ministries of health and defense, national cybersecurity agencies, private technology providers and healthcare professionals; establishing clear governance ensures accountability across this ecosystem.

5. EMERGING TECHNOLOGIES AND THE FUTURE OF BIO-DIGITAL THREATS

As NATO charts its trajectory toward 2030 and beyond, the evolving cyber threat environment demands urgent strategic foresight and innovation. Emerging technologies are transforming the operational, tactical, and strategic dimensions of security in cyberspace, reshaping the nature of threats and the methods required to confront them. This transformation is not merely a technological shift but a structural one, where the very architecture of power, deterrence, and resilience are redefined by innovation. Moreover, the forthcoming transformative technological cycle will be propelled by synthetic biology. Alongside ongoing advancements in associated technological domains (for instance, biodata and biosensors), this trend will elevate concerns such as research security (protecting sensitive research) and regulatory matters to a prominent position. Artificial intelligence, quantum computing, autonomous systems, and the growing interdependence between digital and physical domains converge to create an unstable equilibrium. NATO must prepare for a future in which adversaries exploit speed, ambiguity, and complexity to challenge democratic resilience, strategic cohesion, and military effectiveness (Lucarelli S, 2021). Aside from AI, collaborations between the public and private sectors are crucial to NATO's cybersecurity framework. The private sector, particularly technology firms such as Microsoft, Google, and Cisco, possess the sophisticated technology and threat intelligence capabilities essential for enhancing NATO's defensive stance. This partnership enables NATO to utilize the most effective and up-to-date resources for identifying, alleviating, and addressing threats.

Artificial intelligence (AI) and machine learning (ML) stand at the core of this transformation. These technologies enable faster processing of massive datasets, advanced anomaly detection, predictive threat modelling, and real-time response

automation. While offering remarkable advantages in cyber defense and operational planning, AI also lowers the threshold for executing complex cyberattacks. Adversaries may deploy machine-driven deception, intelligent malware, or autonomous intrusion tools, creating a scenario where human reaction time becomes irrelevant. The danger is not limited to technological superiority but to cognitive asymmetry, where NATO's decision-making processes may lag behind the rapid, AI-enhanced actions of a malicious actor (Ertan A, 2020).

Equally significant is the rise of autonomous and semi-autonomous systems, ranging from unmanned aerial vehicles and robotic platforms to software agents operating in cloud-based infrastructures. These systems increase operational efficiency and reduce human exposure to direct threats, but they also become new targets for cyber intrusion. A compromised autonomous system could be repurposed as a weapon or become part of a coordinated swarm attack. The convergence of autonomy and connectivity introduces vulnerabilities that traditional cybersecurity models are ill equipped to address. The result is a volatile battlespace where the cyber and kinetic realms are increasingly intertwined (Lucarelli S, 2021).

Meanwhile, the rollout of advanced communication's infrastructure, particularly 5G networks, introduces a broader and deeper digital attack surface. 5G enables massive device connectivity and low-latency data exchange, but it also embeds critical dependencies on software-defined functions, cloud integration, and supplier trust. NATO allies must grapple with the geopolitical implications of technology supply chains and the risks of digital dependencies on non-trusted providers. The security of digital infrastructure is no longer purely technical; it is political, strategic, and transnational. Ensuring the integrity and resilience of communication networks is as vital as defending physical territory (Ertan A, 2020).

Quantum computing, while still in its infancy, poses a looming threat to the cryptographic foundations of modern security. Once scalable quantum machines become operational, they could break widely used public-key encryption schemes, undermining secure communications across military, intelligence, and civilian sectors. The race toward quantum-resistant encryption has begun, but NATO must assume a proactive stance. The Alliance's information assurance models must anticipate the "quantum surprise," investing not only in technological adaptation but also in the human and institutional agility to absorb rapid shifts (Zornetta, 2024). Another

domain of rising concern is the explosive growth of cyber-physical systems and the Internet of Things (IoT), particularly within critical infrastructure. From energy grids and water systems to military logistics and healthcare, increasingly connected environments create complex interdependencies. A cyberattack on one node can cascade across systems, causing widespread disruption or even loss of life. The digitization of society and the militarization of connectivity render cybersecurity not only a technical imperative but also a civilizational one. The protection of public trust, democratic governance, and societal functionality becomes part of NATO's strategic calculus (lessing J, 2021).

Regarding bio-digital threats, NATO has established a network of Centers of Excellence. For example, the Joint Chemical Biological Radiological and Nuclear Defense COE is focused on developing standards and knowledge to enhance interoperability and capabilities among member and partner nations, while maintaining close collaboration with other pertinent COEs, such as the Civil-Military COE, to foster synergies between NATO and the EU through dedicated studies. Simultaneously, the Cooperative Cyber Defense COE located in Estonia serves as a multinational and interdisciplinary cyber defense hub, offering research, training, and exercises related to cyber technology, strategy, operations, and law. However, there remains significant potential for improvement, particularly in collaboration with EU organizations and agencies like the EDA (and its Technology & Innovation Unit) to better prepare for future hybrid bio-digital threats, including high-impact, low-probability risks that could affect the health systems of both the EU and NATO.

In light of these developments, NATO's concept of deterrence and defense must evolve. Cyber deterrence is inherently different from nuclear or conventional deterrence. It is more ambiguous, harder to attribute, and often operates below the threshold of open conflict. This requires NATO to develop new models of collective resilience, attribution mechanisms, and credible response postures that align with democratic values and international law. Capacity building, information sharing, and real-time coordination among allies will be the backbone of any effective cyber strategy (Lucarelli S, 2021). Ultimately, NATO must embrace a dynamic, forward-looking cybersecurity agenda rooted in technological literacy, strategic foresight, and institutional adaptability. This includes investing in next-generation cyber capabilities, enhancing interoperability among member states, cultivating a skilled

workforce, and fostering innovation through public-private partnerships. In an era defined by digital disruption, the Alliance's strength will depend not only on its military assets but also on its ability to anticipate, absorb, and respond to complex cyber threats with unity and speed (Ertan A, 2020).

6. DIGITAL HEALTH TRANSFORMATION IN EUROPE: CHALLENGES, STRATEGIC INITIATIVES, AND NATO'S ROLE IN SHAPING THE FUTURE OF HEALTHCARE

The digitalization of health is not a recent development in European healthcare systems. The adoption of information and communications technology (ICT) across public health institutions, including the use of secure digital equipment and licensed software outside core hospital infrastructure, has grown exponentially, particularly under the impact of COVID-19 restrictions. Similar trends observed in both NATO and EU health-related initiatives, as most European health systems currently employ at least some level of digital health technologies and enterprise resource planning (ERP) systems. Many also operate partially digitalized healthcare infrastructures and administrative bodies (Bocean and Vărzaru, 2025).

A small number of EU member states are now striving for more advanced and integrated digital health ecosystems, including real-time data exchange platforms and comprehensive command, control, communications, intelligence, surveillance, and response (C4ISR) systems for health crises. For instance, the United Kingdom is developing a unified and secure 'Digital Backbone' for its National Health Service (NHS), supported by initiatives such as the 'Digital Foundry' and a dedicated 'Digital Function' for healthcare management. This digital transfo-rmation aims to replace thousands of outdated legacy systems and applications, serving over 200,000 healthcare personnel across clinical, administrative, and logistical functions. The 2022 Plan for Digital Health and Social Care, along with subsequent health digitalization strategies, reaffirm the UK's commitment to accelerating this shift towards a fully integrated digital infrastructure (M. Honeyman, 2020; Värri, 2020). Similarly, France has established the Health Data Hub (HDH), a national platform designed to facilitate secure and unified access to health data for research and innovation purposes. The HDH aims to consolidate various health databases, enhancing the country's capacity for data-driven healthcare solutions and fostering digital sovereignty in the health sector. This initiative reflects France's commitment to developing a robust

digital backbone for its national health infrastructure (Szeftel *et al.*, 2025). Furthermore, countries such as Estonia, Finland, Italy, the Netherlands, Norway, Spain, and Sweden have also made significant strides in integrating digital technologies into their healthcare systems. For instance, Estonia's implementation of the X-Road platform has enabled seamless interoperability between various health services, while Finland's Digital Health Village provides a comprehensive online portal for patient care. These advancements often involve collaborations with private-sector technology providers, adopting models based on data-, software-, and infrastructure-as-a-service to enhance efficiency and accessibility in healthcare delivery (Vaagan RW, 2021). However, European nations still face substantial obstacles in fully digitalizing their healthcare infrastructures. Most lack fully integrated digital health data management systems or are still in the process of developing them. Many rely on outdated, localized data-storage systems located on-site within hospitals or clinics. Additionally, a large proportion of EU member states struggle to maintain and regularly update their digital health systems. In some cases, security-critical systems have not been upgraded for over a decade, creating major vulnerabilities (Majcherek *et al.*, 2024).

The use of cloud-based healthcare services remains very limited in Europe, with only a few countries, such as France, Germany, and the UK, employing health cloud services at a national level or within federated networks. Although the European Health Fund (hypothetically adapting the EDF) supports projects aimed at cloud-based storage and collaborative digital health networks, less than 1% of cloud-service providers in Europe are European-based companies, raising critical concerns around data sovereignty. Indeed, data sovereignty remains a foundational principle of digital transformation across both EU and NATO health strategies. Despite the availability of technical solutions to safeguard data integrity and ownership, cross-border and cross-sectoral data sharing remains a medium-term challenge for both organizations. For instance, many European health institutions still rely on manual systems for logging staff capacity and equipment readiness. Delays in reporting and updating records on the maintenance of critical medical equipment are common. A recent example is the widespread difficulty EU members faced in providing real-time updates on medical supplies and pharmaceuticals during joint procurement efforts, an initiative that aimed to strengthen EU solidarity in response to the war in Ukraine and its humanitarian health impacts

(Burkadze, 2022; Jain *et al.*, 2022; Kitsos and Pappa, 2024).

7. DIGITAL HEALTH TRANSFORMATION IN EUROPE: THE ROLE OF NATO AND THE EU IN SHAPING SOVEREIGN HEALTH SYSTEMS

While European countries are progressively increasing investments in digital health infrastructure, available data show that healthcare spending specifically allocated to digital transformation, including enterprise IT systems and cybersecurity, remains relatively low compared to total healthcare budgets. Estimates suggest that digital health spending as a share of healthcare budgets among selected European countries ranges between approximately 0.4% and 8.3%. According to Statista (2024), the digital health market in the United Kingdom was valued at around $5.55 billion in 2024, while in France; it projected to reach approximately €3.75 billion. Spain, by contrast, allocates only about 0.4% of its health budget to digital transformation efforts, trailing behind Italy and Germany (Gallo *et al.*, 2021; Weresa, Ciecierski and Filus, 2024; Statista, 2025). Cross-national cost comparisons are inherently difficult due to the lack of standardized, transparent reporting. Most European governments do not publish separate budget lines for software, IT, and digital service expenditures, complicating efforts to track spending across investment, maintenance, and system decommissioning categories (Frintrup, Schmidthuber and Hilgers, 2022). For instance, the UK's 2023 health transformation plan allocated $5.55 billion for digital upgrades, yet previous estimates from 2019 suggested that replacing six major legacy systems in the National Health Service (NHS) could cost as much as $14.1 billion over the subsequent decade. While it remains unclear whether current annual budgets include costs for ongoing maintenance and decommissioning, some countries, such as France, Italy, and Spain, do distinguish these elements in their financial reporting. Accurate assessments are further impeded by inconsistent disclosure and insufficient granularity in national health budgets. Nevertheless, understanding how nations invest in healthcare digitalization is essential to tracking their progress toward robust, tech-enabled health systems (Frintrup, Schmidthuber and Hilgers, 2022; Damar, Özen and Yılmaz, 2024; (Russell, Bukhari and Galloway, 2019; Galea and Abdalla, 2023; Karaferis, Aletras and Niakas, 2023;).

Notably, the financial structure of digital transformation differs significantly from that of traditional healthcare infrastructure procu-

rement. In digital health, investment and maintenance costs balanced over time. In contrast, traditional medical infrastructure involves high up-front procurement costs but lower long-term upkeep. There is growing recognition that public healthcare systems across Europe lag significantly behind the private sector, especially the tech industry, in fully leveraging data as a strategic asset for value creation and improved outcomes. Industry stakeholders emphasize that digital transformation typically requires three to four years to yield operational results, depending on the complexity and scale of the project. However, outdated procurement models and inflexible budgetary frameworks often result in long-term initiatives that span decades rather than years. For example, digital health projects in Germany, Italy, and Spain are not expected to conclude before 2030 or 2035. Similarly, Norway anticipates a decade-long timeline for its national digital health overhaul. By contrast, digital transformation in leading industrial sectors often occurs within a two-year window. The urgency to accelerate digital health reform has intensified in the wake of COVID-19 and other health crises, which demonstrated the need for rapid transitions from concept to deployment. For example, during emergencies, health technologies such as digital contact tracing, AI-powered diagnostics, and telemedicine platforms were developed and deployed within weeks. Yet these rapid-cycle innovations remain the exception rather than the rule across European health systems (Gopal et al., 2019; Karaferis D, Balaska D and Pollalis Y, 2024; Brunetti et al., 2020; Karaferis, Balaska and Pollalis, 2024; Dimitris, Dimitra and Yannis, 2025; Pérez Sust et al., 2020; Raja et al., 2023;).

In July 2023, Germany's Chief of Defense (in a parallel domain) acknowledged that traditional procurement and innovation cycles are ill suited to the fast-paced evolution of new technologies. Similar critiques have emerged from within the UK healthcare sector, where the 2023 Health Command Paper committed to reducing the time between identifying a clinical or technological need and the full-scale deployment of a digital solution. The paper proposed a maximum of three years for health-related digital programs, a goal more moderate than some had hoped but still a significant improvement over historical timeline. Across NATO and EU health and emergency response systems, digital health programs that move from initial conception to operational implementation within months remain rare. Bridging this gap is essential for achieving digital sovereignty, operational agility, and improved patient care across

Europe (Begkos, Antonopoulou and Ronzani, 2024; Frassini, 2024).

8. CONCLUSIONS

The evolving security environment of the 21st century challenges traditional defense paradigms by highlighting the convergence of digital, biological, and hybrid threats. As pandemics, cyberattacks, disinformation campaigns, and the weaponization of health infrastructure intersect; it becomes clear that security extends beyond the battlefield into the realms of data, health, and trust. Both NATO and the European Union (EU) must adapt their defense strategies to address these emerging complexities on exploration of dual-use technology (for both military and civilian purpose) for the overall benefit of our societies.

Health intelligence (HI), once considered a peripheral aspect of defense planning, has become an essential strategic asset. The COVID-19 pandemic revealed the vulnera-bilities of isolated systems, the impact of delayed coordination, and the lack of preparedness for bio-digital threats. However, it also underscored the importance of data-driven insights, international collaboration, and adaptive digital tools that, when deployed strategically, can significantly enhance defense capabilities.

Digital transformation in defense must go beyond merely adopting new technologies; it must foster a fundamental shift in mindset, operational strategies, and inter-institutional cooperation. This transformation involves incentivized private R&D, modernizing infrastructures, enhancing cyber resilience, embedding foresight, interoperability, and real-time responsiveness into strategic frameworks. NATO and the EU must work towards creating agile systems capable of functioning seamlessly across civil-military boundaries, ensuring that health systems and data ecosystems integrated into the concept of critical infrastructure alongside energy and transport systems.

Incorporating health intelligence into NATO and EU defense strategies allows for the transition from reactive responses to proactive preparedness. It is vital to align national and supranational strategies, dismantling barriers between public health, national defense sector and enterprises in health industry (including innovative SMEs). This approach not only addresses immediate threats but also prepares for future risks, enhancing the resilience and readiness of both organizations. The successful defense strategies of the future will require more than the ability to deter and defeat threats, they must anticipate and mitigate risks before they materialize. Health intelligence must be viewed as a central pillar

of this strategic foresight. This approach will not only strengthen the transatlantic alliance's resilience but also reinforce the values of trust, solidarity, and collective security in the digital era. Ultimately, the integration of health, digital innovation, and defense strategy is both an operational necessity and a political and ethical imperative. The decisions made today will shape the security landscape of tomorrow. NATO and the EU must lead this transformation with urgency, vision, and unity.

While this paper provides an initial exploration of health intelligence integration, further research is required to address implementation challenges. Future studies should examine procurement models and decision-making frameworks for defence planners, develop assessment tools for measuring integration readiness, and explore the privacy, legal and ethical implications of cross-border health data sharing (Gerke, Minssen and Cohen, 2020). Engaging practitioners will be essential for identifying solutions that are technologically feasible, ethically sound and sensitive to organisational cultures. Such work will ensure that health intelligence integration delivers tangible policy impact and supports transatlantic security.

In conclusion, the integration of Health Intelligence (HI) into NATO's broader defense strategy marks a pivotal shift in how security is conceptualized and operationalized in the digital age. As modern warfare becomes multidimensional, enco-mpassing biosecurity risks, digital vulnerabilities, and societal fragilities, health must be embedded as a central element of defense and resilience. While the focus of European defense ministries remains on defense innovation and emerging technologies like artificial intelli-gence (AI), it is the secure, interoperable digital transformation of data that will underpin NATO and EU military power in the future. For effective and impactful digital transformation, NATO and the EU must establish coherent, secure digital infrastructures that promote cross-border interoperability and human-centric designs. The rapid pace of technological advancement makes it essential to act quickly, as the race against evolving threats is both strategic and existential. Health intelligence plays a crucial role as a preventive mechanism and strategic asset by bridging civil and military preparedness, supporting early warning systems, protecting force health, and reinforcing societal trust in institutions. Building a resilient, secure, and technologically advanced European defense requires more than investing in hardware and algorithms. It demands a fundamental shift in mindset, with digital transformation

and health intelligence serving as foundational pillars of NATO and EU strategic readiness.

Declaration of Interest: The authors declare no conflict of interest.

Ethical approval: The ethical approval was not required, as the study conducted did not involve any ethical concerns or issues.

Funding: None.

Author's contribution: All authors were involved in all steps for preparation of this article, including final proofreading and gave final approval of the version to be published.

REFERENCES

[1] Andrea Gilli. *NATO-Mation: Strategies for Leading in the Age of Artificial Intelligence*. Rome; 2020 Dec.

[2] Anghel V, Jones E. Is Europe really forged through crisis? Pandemic EU and the Russia – Ukraine war. *J Eur Public Policy*. 2023 Apr 3;30(4):766–86.

[3] Bachmann SD. Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats - mapping the new frontier of global risk and security management. *Amicus Curiae*. 2012 Jun 28;2011(88).

[4] Baroncelli S. Recovery and Resilience Facility. In: *Research Handbook on Post-Pandemic EU Economic Governance and NGEU Law*. Edward Elgar Publishing; 2024. p. 110–27.

[5] Begkos C, Antonopoulou K, Ronzani M. To datafication and beyond: Digital transformation and accounting technologies in the healthcare sector. *The British Accounting Review*. 2024 Jul;56(4):101259.

[6] Bente BE, Van Dongen A, Verdaasdonk R, van Gemert-Pijnen L. eHealth implementation in Europe: a scoping review on legal, ethical, financial, and technological aspects. *Front Digit Health*. 2024 Mar 8;6.

[7] Bocean CG, Vărzaru AA. Health status in the era of digital transformation and sustainable economic development. *BMC Health Serv Res.* 2025 Mar 5;25(1):343.

[8] Bowsher G, Milner C, Sullivan R. Medical intelligence, security and global health: the foundations of a new health agenda. *J R Soc Med*. 2016 Jul; 109(7):269–73.

[9] Bricknell M., Gad M, Homan Z, Gheorghe A, Quirk E, Kazibwe J. An analysis of the national responses to the COVID-19 pandemic through the lens of medical military support requirements [*Internet*]. Norfolk, Virginia; 2020 [cited 2025 Sep 7]. Available from: https://kclpure.kcl.ac.uk/portal/en/publications/an-analysis-of-the-national-responses-to-the-covid-19-pandemic-th

[10] Brunetti F, Matt DT, Bonfanti A, De Longhi A, Pedrini G, Orzes G. Digital transformation challenges: strategies emerging from a multi-stakeholder approach. *The TQM Journal*. 2020 Jul 21;32(4):697–724.

[11] Burkadze K. Trends of Digital Transformation Based on the UN, EU, and NATO Experiences.

Fletcher F World Aff. 2022;46(111).

[12] Burwell FG; PK. *Atlantic Council, Europe Center*. 2022 [cited 2025 Sep 7]. Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy. Available from: https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-in-practice-the-eus-push-to-shape-the-new-global-economy/

[13] Burwell FG; PK. The European Union and the search for digital sovereignty: building "Fortress Europe" or preparing for a new world? [*Internet*]. Washington, DC; 2020 Jun [cited 2025 Sep 7]. Available from: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/

[14] Caliskan M, Liégeois M. The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials. *Small Wars & Insurgencies*. 2021 Feb 17;32(2):295–319.

[15] Cannon S. *JAPCC Journal, Edition 37*, Leadership Perspective. 2024 [cited 2025 Sep 7]. The Alliance's Transition to Multi-Domain Operations: An AIRCOM Perspective. Available from: https://www.japcc.org/articles/the-alliances-transition-to-multi-domain-operations/

[16] Crespi F, Caravella S, Menghini M, Salvatori C. European Technological Sovereignty: An Emerging Framework for Policy Strategy. *Intereconomics*. 2021 Nov 11;56(6):348–54.

[17] Csernatoni R, Martins BO. Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination. *Geopolitics*. 2024 May 26;29(3):849–72.

[18] Damar M, Özen A, Yılmaz A. Cybersecurity in The Health Sector in The Reality of Artificial Intelligence, And Information Security Conceptually. *Journal of AI*. 2024 Dec 31;8(1):61–82.

[19] Dimitris K, Dimitra B, Yannis P. Digitalization and Artificial Intelligence as Motivators for Healthcare Professionals. *Japan Journal of Research.* 2025 Jan 1;6(3).

[20] Erondu NA, Rahman-Shepherd A, Khan MS, Abate E, Agogo E, Belfroid E, et al. Improving National Intelligence for Public Health Preparedness: a methodological approach to finding local multi-sector indicators for health security. *BMJ Glob Health*. 2021 Jan;6(1):e004227.

[21] Ertan A FKPPST. Cyber Threats and NATO 2030: Horizon Scanning and Analysis [Internet]. Tallinn, Estonia: *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE); 2020 [cited 2025 Sep 7]. Available from: https://www.ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

[22] Fahy N MNPD. European support for improving health and care systems [Internet]. Copenhagen (Denmark): *European Observatory on Health Systems and Policies*; 2021.

[23] Fasola N. Reforming and Enhancing Partnerships to Strengthen NATO's Strategic Posture. *The US Army War College Quarterly: Parameters*. 2024 Nov 21;54(4).

[24] Fiott D. *European Union Institute for Security Studies*. 2020 [cited 2025 Apr 25]. Digitalising defence: Protecting Europe in the age of quantum computing and the cloud. Available from: https://www.iss.europa.eu/content/digitalising-defence

[25] Fiott D. In every crisis an opportunity? European Union integration in defence and the War on Ukraine. *J Eur Integr*. 2023 Apr 3;45(3):447–62.

[26] for different actors. e-Estonia guide: the most advanced digital society in the world. Tallinn: Enterprise Estonia [Internet]. 2025 [cited 2025 Sep 7]. Available from: https://e-estonia.com/wp-content /uploads/eestonia_guide_08-04-2025 .pdf#:~:text=online%E2%80%93it%20takes%20only%203%20minutes%21

[27] Frassini J. CIV-MIL integration in the transformation of the EU healthcare network: a dual-gain strategy. *Journal of Integrated Care*. 2024 Aug 8;32(3):252–69.

[28] Frintrup M, Schmidthuber L, Hilgers D. Towards accounting harmonization in Europe: a multinational survey among budget experts. *International Review of Administrative Sciences*. 2022 Jun 27;88(2):390–410.

[29] Gaeta E, Salman Haleem M, Lopez-Perez L, Manea M, Fernanda Cabrera Umpierrez M, Teresa Arredondo Waldmeyer M, et al. GATEKEEPER Platform: Secure Processing Environment for European *Health Data Space. IEEE Access*. 2025;13:34627–38.

[30] Galea S, Abdalla SM. Data to Improve Global Health Equity—Key Challenges. *JAMA Health Forum*. 2023 Nov 2;4(11):e234433.

[31] Gallo F, Seniori Costantini A, Puglisi MT, Barton N. Biomedical and health research: an analysis of country participation and research fields in the EU's Horizon 2020. *Eur J Epidemiol*. 2021 Dec 17;36(12):1209–17.

[32] Gendy MEG, Yuce MR. Emerging Technologies Used in Health Management and Efficiency Improvement During Different Contact Tracing Phases Against COVID-19 Pandemic. *IEEE Rev Biomed Eng*. 2023;16:38–52.

[33] Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. In: *Artificial Intelligence in Healthcare*. Elsevier; 2020. p. 295–336.

[34] Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. In: *Artificial Intelligence in Healthcare*. Elsevier; 2020. p. 295–336.

[35] Gopal G, Suter-Crazzolara C, Toldo L, Eberhardt W. Digital transformation in healthcare – architectures of present and future information technologies. *Clinical Chemistry and Laboratory Medicine (CCLM).* 2019 Feb 25;57(3):328–35.

[36] Grgić G. Redefining NATO's Indo-Pacific partnerships: cooperative

security meets collective defence and deterrence. *Asian Security*. 2024 Jan 2;20(1):39–55.

[37] Haby MM, Chapman E, Barreto JOM, Mujica OJ, Rivière Cinnamond A, Caixeta R, et al. Greater agreement is required to harness the potential of health intelligence: a critical interpretive synthesis. *J Clin Epidemiol*. 2023 Nov;163:37–50.

[38] Haddud A, McAllen D. Digital Workplace Management: Exploring Aspects Related to Culture, Innovation, and Leadership. In: *2018 Portland International Conference on Management of Engineering and Technology (PICMET). IEEE*; 2018. p. 1–6.

[39] Honeyman MMDEHDA. *Public Health Wales NHS Trust (Research and Evaluation Division)*. 2020 [cited 2025 Sep 7]. Digital technology and health inequalities: a scoping review. Available from: https://phw.nhs.wales/publications/publications1/digital-technology-and-health-inequalities-a-scoping-review/

[40] Ilangakoon TS, Weerabahu SK, Samaranayake P, Wickramarachchi R. Adoption of Industry 4.0 and lean concepts in hospitals for healthcare operational performance improvement. *International Journal of Productivity and Performance Management*. 2022 Jun 24;71(6):2188–213.

[41] J.Metsallik, P. Ross, D. Draheim, G. Piho. Ten Years of the e-Health System in Estonia. In: Adrian Rutle (Western Norway University of Applied Sciences BNYL (Western NU of ASBNWM (St. FXUACLI (Gran SSILI, editor. *Proceedings of the 3rd International Workshop on (Meta) Modelling for Healthcare Systems (MMHS 2018)* [Internet]. Bergen, Norway: CEUR Workshop Proceedings (CEUR-WS); 2018 [cited 2025 Sep 7]. p. 6–15. Available from: : ceur-ws.org/Vol-2336/MMHS2018_invited.pdf.

[42] Jain N, Prasad S, Bordeniuc A, Tanasov A, Shirinskaya AV, Béla B, et al. European Countries Step-up Humanitarian and Medical Assistance to Ukraine as the Conflict Continues. *J Prim Care Community Health*. 2022 Jan 23;13.

[43] Karaferis D, Aletras V, Niakas D. Job satisfaction of primary healthcare professionals: a cross-sectional survey in Greece. *Acta Biomed*. 2023 Jun 14;94(3):e2023077.

[44] Karaferis D, Balaska D, Pollalis Y. Enhancement of Patient Engagement and Healthcare Delivery Through the Utilization of Artificial Intelligence (AI) Technologies. *Austin Journal of Clinical Medicine*. 2024 Nov 15;9(2).

[45] Karaferis DC, Niakas DA. Exploring Inpatients' Perspective: A Cross-Sectional Survey on Satisfaction and Experiences in Greek Hospitals. *Healthcare*. 2024 Mar 14;12(6):658.

[46] Karaferis Dimitris BD and PY. Artificial Intelligence and Robotics:Catalysts or Threats in the Development of Healthcare. *Biostat Biom Open Access J* . 2024;11(5).

[47] Kitsos P, Pappa P. Cloud Governance in the European Union: Unlocking the Power of Data in the Era of the Digital Economy. In 2024. p. 99–114.

[48] Lantzsch H, Eckhardt H, Campione A, Busse R, Henschke C. Digital health applications and the fast-track pathway to public health coverage in Germany: challenges and opportunities based on first results. *BMC Health Serv Res*. 2022 Sep 21;22(1):1182.

[49] Blessing J KEKEPNM (editors); TR (associate editor). NATO 2030: Towards a New Strategic Concept and Beyond [Internet]. *Henry A. Kissinger Center for Global Affairs*; Johns Hopkins SAIS; DAAD (German Academic Exchange Service); 2021 [cited 2025 Sep 7]. Available from: https://sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond

[50] Lucarelli S MAMF. NATO Decision-Making in the Age of Big Data and Artificial Intelligence. In NATO Allied Command Transformation; *University of Bologna; Istituto Affari Internazionali (IAI)*; 2021 [cited 2025 Sep 7]. Available from: https://www.iai.it/sites/default/files/978195445000.pdf (iai.it)

[51] Madiega TA. European Parliamentary Research Service (EPRS). 2020 [cited 2025 Sep 7]. *Digital sovereignty for Europe*. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[52] Majcherek D, Hegerty SW, Kowalski AM, Lewandowska MS, Dikova D. Opportunities for healthcare digitalization in Europe: Comparative analysis of inequalities in access to medical services. *Health Policy* (New York). 2024 Jan; 139:104950.

[53] Mauro M, Noto G, Prenestini A, Sarto F. Digital transformation in healthcare: Assessing the role of digital technologies for managerial support processes. *Technol Forecast Soc Change*. 2024 Dec; 209:123781.

[54] Mesterhazy A. The Role of NATO's Armed Forces in the COVID-19 Pandemic [Internet]. 2020 Jun [cited 2025 Sep 7]. Available from: https://www.nato-pa.int/download-file?filename=%2Fsites%2Fdefault%2Ffiles%2F2020-06%2F091%20DSC%2020%20E%20-%20COVID-19%20SPECIAL%20REPORT_1.pdf

[55] NATO Allied Command Transformation. Empowering NATO's Multi-Domain Operations Through Digital Transformation [Internet]. 2023 [cited 2025 Sep 7]. Available from: https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/

[56] NATO Reflection Group. NATO. 2020 [cited 2025 Sep 7]. NATO 2030: Unity for a New Era – Reflection Group Final Report. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

[57] NATO STO SET Panel. NATO Research Lecture Series SET-290: Artificial Intelligence for Military Multiple Sensor Fusion Engines. In: *NATO Science & Technology Organization (STO), Systems and Electronics Technology (SET) Panel* [Internet]. Rome, Wachtberg,

Budapest: Lecture Series Programme; 2022 [cited 2025 Sep 7].
[58] NATO. NATO official text. 2024 [cited 2025 Sep 7]. NATO's Digital Transformation Implementation Strategy. Available from: https://www.nato.int/cps/en/ natohq/official_texts_229801.htm#:~:text=Strategic%20 Outcomes
[59] NATO. NATO. 2022 [cited 2025 Sep 7]. Summary of NATO's Data Exploitation Framework Policy (DEFP). Available from: https://www.nato.int/cps/en/natohq/official_texts_210002.htm
[60] NATO's strategy for digital transformation [Internet]. 2024 [cited 2025 Sep 7]. Available from: https://www.nato.int/cps/en/natohq/news_229985.htm
[61] Niño Sevilla Palma F. Digital Health Beyond Borders: Interoperability Challenges and Critical Success Factors in the Deployment of Cross-border ePrescription in Finland and Estonia. *Westfälische Wilhelms-Universität Münster*; 2021.
[62] Oberländer M, Beinicke A, Bipp T. Digital competencies: A review of the literature and applications in the workplace. *Comput Educ.* 2020 Mar; 146:103752.
[63] Odone A, Buttigieg S, Ricciardi W, Azzopardi-Muscat N, Staines A. Public health digitalization in Europe. *Eur J Public Health*. 2019 Oct 1;29(Supplement_3):28–35.
[64] Orăștean R, Sava R, Mărginean S. Measuring Healthcare Digitalisation in The European Union: Trends and Challenges. *Rev Econ.* 2022 dec 20;74(4):64–74.
[65] Pérez Sust P, Solans O, Fajardo JC, Medina Peralta M, Rodenas P, Gabaldà J, et al. Turning the Crisis Into an Opportunity: Digital Health Strategies Deployed During the COVID-19 Outbreak. *JMIR Public Health Surveill*. 2020 May 4;6(2):e19106.
[66] Policy Department DG for EP of the U. How the COVID-19 crisis has affected security and defence-related aspects of the EU [Internet]. 2021 Jan [cited 2025 Sep 7]. Available from: https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2021)653623
[67] Raja M, Kymre IG, Bjerkan J, Galvin KT, Uhrenfeldt L. National digital strategies and innovative eHealth policies concerning older adults' dignity: a document analysis in three Scandinavian countries. *BMC Health Serv Res.* 2023 Aug 10;23(1):848.
[68] Rauch TM, Daniel JC, Erickson EA, Shiau D, Cincotta J V. US Department of Defense Global Health Engagement: supporting global health security, readiness and interoperability. *BMJ Mil Health.* 2024 Jul;170(e1):e1–3.
[69] Ruohonen J, Timmers P. Early Perspectives on the Digital Europe Programme. 2025 Jan 6;
[70] Russell MD, Bukhari M, Galloway J. The price of good health care. *Rheumatology*. 2019 Jun 1;58(6):931–2.
[71] Shea J. How is NATO Meeting the Challenge of Cyberspace. ImprintPRISM: *A Journal of the Center for Complex Operations*. 2017 Dec;7(2):18–29.

[72] Soare S. International Institute for Strategic Studies (IISS). 2023 [cited 2025 Sep 7]. Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age. Available from: https://www.iiss.org/research-paper/2023/08/digitalisation-of-defence--in-nato-and-the-eu/

[73] Statista. Statista Health Market Outlook. 2025 [cited 2025 Sep 7]. Revenue in the digital health market in the United Kingdom. Available from: https://www.statista.com/forecasts/1436300/revenue-digital-health-digital-health-market-united-kingdom

[74] Sylvia N. Emerging Insights Royal United Services Institute for Defence and Security Studies. 2025 [cited 2025 Sep 7]. European Digital Defence Priorities in an Uncertain World. Available from: https://static.rusi.org/european-digital-defence-priorities-march-2025.pdf

[75] Szeftel D, Jouhet V, Duluc G, Charle-Maachi C, Sejourné T, Fabiano J, et al. Health data: Regionalised access is a priority challenge for building a secure, transparent and innovative national health data repository. *Therapies*. 2025 Jan;80(1):125–34.

[76] Vaagan RW TSSAFJLA. A Critical Analysis of the Digitization of Healthcare Communication in the EU: A Comparison of Italy, Finland, Norway, and Spain. *Int J Commun* [Internet]. 2021 Mar 27 [cited 2025 Sep 7];1718–40. Available from: https://ijoc.org/index.php/ijoc/article/view/15399

[77] Värri AJDPGJDMHKHUMK and LPH. Integrated Citizen Centered Digital Health and Social Care [Internet]. 1st ed. Vol. 12. SAGE; 2020 [cited 2025 Sep 7]. Available from: https://www.perlego.com/book/5032898/integrated-citizen-centered-digital-health-and-social-care-citizens-as-data-producers-and-service-cocreators-pdf

[78] Veronesi G, Kirkpatrick I, Altanlar A, Sarto F. Corporatization, Administrative Intensity, and the Performance of Public Sector Organizations. *Journal of Public Administration Research and Theory*. 2023 Sep 12;33(4):701–15.

[79] Weresa MA, Ciecierski C, Filus L. Digitalization and Innovation in Health. London: Routledge; 2024.

[80] Wolff AT. Who Is NATO for? In: *The Oxford Handbook of NATO*. Oxford University Press; 2025. p. 77–93.

[81] Zorloni L. Europe Is Pumping Billions Into New Military Tech [Internet]. 2024 [cited 2025 Sep 7]. Available from: https://www.wired.com/story/european-commission-military-tech-spending/

[82] Zornetta A. Quantum-safe global encryption policy. *International Journal of Law and Information Technology.* 2024 Jun 1;32.