EUROPE, A SECURE & DIGITAL POWERHOUSE

© AI-generated cover photo by Victoria Bonefeld Dahl

Recommendations for the digitalisation of defence

DIGITALEUROPE

The very fabric of European security has been shaken by Russia's aggression in Ukraine.

This brutal act of war has shattered a long-held illusion of peace and underscored the stark reality: Europe must take a more proactive and unified role in its own defence.

Foreword

This report arrives at a critical juncture. It doesn't merely explore the potential of digital technologies in defence – it champions it.

Both the EU and NATO have designated certain emerging and disruptive technologies as critical to our security.[1] Both have also piloted new funding schemes to promote early-stage innovators.

As a member of the Advisory Group to the Secretary General of NATO on Emerging and Disruptive Technologies, I've witnessed first-hand the transformative power of digital innovation in defence. Seeing NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund (NIF) take off fills me with pride.

It is a testament to joint action, embodying both the strength of collaboration and the transformative power of innovation for our collective defence.

However, DIANA and NIF are just the beginning. The challenges Europe is facing demand a truly European response. We can and must do more. In our recent manifesto, we called for a 25% funding target for digital across EU and NATO funds.[2]

A digital watershed is needed, a moment where we break free from fragmented efforts and embrace a European approach to fostering dual-use technological innovation. Relying solely on reactive measures like export controls and investment screening is insufficient. By the time investigations are complete, valuable IP may already be in the wrong hands. We must offer our most valuable companies attractive incentives to collaborate, including direct buyouts or strategic partnerships. By presenting a clear win-win scenario, we can give friendly companies an immediate option to join the 'right side of history.'

Imagine a stronger European Investment Fund (EIF), with a reinforced mandate to support the development of cutting-edge technologies that have both civilian and military applications. Imagine a network of European innovation hubs, fostering collaboration and knowledge transfer across borders. Imagine a Europe where we coordinate tax incentives on critical technologies. This is the future we must build.

Finally, whilst Member States collectively spend €240 billion on defence procurement, procurement schemes are highly nationalised.[3] Transitioning to a system of EU-wide funding will help defragment the EU's capabilities.

This report serves as a roadmap towards that future. It details the immense potential of digital technologies to reinforce European defence – from enhanced battlefield awareness to sophisticated cyber resilience. But it goes beyond mere technology. It emphasises the need for a strategic shift, a shared EU vision that leverages our collective strengths.

The time for complacency is over. Member States are called upon to act with urgency and unity. Let this report be a catalyst, a rallying cry for a more robust, digitally powered EU defence. Let us rise to this challenge, for the sake of our continent and the security of generations to come.

Cecilia Bonefeld-Dahl
Director General
DIGITALEUROPE

[1] See https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4735 and https://www.nato.int/cps/en/natohq/topics_184303.htm, respectively.
[2] See DIGITALEUROPE, Europe 203: A digital powerhouse, available at https://cdn.digitaleurope.org/uploads/2023/11/DIGITALEUROPE-EUROPE-2030-A-DIGITAL-POWERHOUSE-FINAL_DECEMBER_WEB.pdf.
[3] EDA Defence Data 2022, available at https://eda.europa.eu/docs/default-source/brochures/2022-eda_defencedata_web.pdf.

Table of Contents

Executive summary

Europe's worsening security landscape demands a new approach. A critical weapon now exists to address evolving threats and complex operational environments – not a new type of gun, tank or plane, but digital innovation.

Digital technologies are key in transforming the EU's defence capabilities. From advanced data analysis and AI to secure communication networks, these innovations offer a powerful toolkit for fortifying Europe's security and defence.

Among others, the recent conflict in Ukraine illustrates how governments and technology providers can work together.[4] Ukraine's tech-savvy population and flexible approach allowed for rapid integration of commercially available technologies. Cloud-based solutions and off-the-shelf tools played a vital role in their defence strategy, demonstrating the effectiveness of digital innovation in real-world security situations. Their Diia e-government tool is also a vital part of the war effort, with functionalities allowing citizens to report enemy troop movements via the same app they have with their ID documents.

"In the struggle between democracy and autocracy, the digital sphere is not a sideshow, but it is the front line."[5]

President Von Der Leyen, 2022

[4] A full analysis of Ukraine's defences goes beyond digital capabilities, including defence readiness, preparation, infrastructures protection and resilience. These are outside the scope of this paper.
[5] Keynote address by President von der Leyen at the Tallinn Digital Summit, available at https://ec.europa.eu/commission/presscorner/detail/en/speech_22_6063.

Europe can harness this same power, if it focuses on three key areas

Investment and collaboration: We must have a 25% allocation for digital across EU and NATO funds, fostering a common use of new technologies in defence. Additionally, proactive incentives like tax deductions for collaborative digital development will stimulate innovation and time-to-market.

A unified EU defence market: Fragmented national procurement schemes hinder progress. We must have an EU-wide approach, leveraging economies of scale and fostering a robust EU digital ecosystem. The recent EDIRPA initiative is a positive step, but more is needed to realise Europe's full potential.

Standardisation and interoperability: Disparate digitalisation levels across Member States create interoperability issues. Expanding the Commission's High-Level Forum on European Standardisation to cover dual-use technologies can streamline standardisation efforts and help achieve real scale.

Through vivid examples, this paper highlights the potential of digital for defence, as well as describing some of the challenges that we face to reach our goal. By embracing collaboration, addressing key challenges and learning from successful examples, the EU can leverage the power of technology to build a more secure and agile defence force, prepared for the threats of tomorrow.

Chapter 1: Key drivers of digital transformation

The full-scale invasion of Ukraine in 2022 has amplified five trends that have been acting as drivers of the digital transformation in our armed forces:

Shift from public to private sector as main military innovators

Previously, it was large government programmes that produced military innovation and then the technologies spilled down to the private sector. Increasingly, the trend is that this process now works rather in reverse: governments and militaries are now reckoning with private tech innovation.

This entails different processes and priorities, and working with non-traditional players. It also requires regular and meaningful dialogue between public and private sectors, and increased investments specifically towards dual-use goods.

An increasingly unpredictable and complex battlefield

Since the outbreak of the conflict, Russia has waged hybrid warfare, mixing irregular forces, cyberattacks, misinformation campaigns and unconventional tactics alongside conventional military operations. Ukraine's response has been just as if not more innovative, mobilising its people at all levels, including former tech workers and ordinary citizens.

For example, using the e-government app Diia, citizens can deliver vital battlefield intelligence on enemy troop movements or missile launches straight to the armed forces.[6] Allied military strategies can also adapt, harnessing new technologies and prioritising efficient information transfer.

[6] https://www.kyivpost.com/post/30149.

The rise of cyberwarfare

Unprecedented numbers of cyberattacks targeting critical infrastructure and government systems have led to increased investment in cybersecurity measures and the development of offensive cyber capabilities by various militaries.

Multi-domain operations (those combining land, air, sea, space and cyberspace) are especially challenging. Effective cyber defence requires clear lines of cooperation, interoperability, hyper-connectivity, common standards and access to the latest innovations and capabilities, which are mostly held by the private sector.

Increased pressure on production

For decades, Europe's decision to shutter domestic mining operations and relocate production facilities to lower-wage regions outside the EU has created a vulnerability: limited access to critical raw materials and essential capabilities within key production processes. This, in turn, hinders efforts to strengthen our defence capabilities.

As Europe needs to boost capacity across the board, the defence sector, like others, is undergoing a digital transformation in its production processes. By leveraging advanced technologies such as digital twins, manufacturers can achieve greater precision, agility and cost-effectiveness throughout the production lifecycle. Furthermore, they can facilitate seamless integration and collaboration across the entire supply chain, enabling manufacturers to achieve greater transparency, flexibility and responsiveness, as in other domains.

Tech diplomacy and increased focus on economic security

The EU, United States, Japan and NATO have all designated certain critical technologies that are essential for the long-term health of their economies. COVID was a wake-up call, exposing the delicate supply chain for microchips.

Given that some of these technologies are dual use, there is a clear and obvious link to national security. Taking the EU as an example, a new strategy is now in place to ensure the development of these technologies is promoted.[7]

[7] See DIGITALEUROPE, *The Download: The EU's Economic Security Strategy*, available at https://www.digitaleurope.org/resources/the-download-the-eus-economic-security-strategy/.

Chapter 2:
10 technologies that will shape our security for the next decade

Artificial intelligence (AI) and big data:

Using sophisticated algorithms to analyse vast datasets, can help uncover hidden patterns that might indicate an impending attack. This proactive approach is similar to what financial institutions use to detect fraud. In aircraft, advanced data-gathering systems can collect significant amounts of data to support rapid decision-making in the cockpit and be passed back down to ground forces.

With the processing power of AI data accelerators, military researchers could unlock solutions to complex challenges at a pace previously unimaginable, e.g. protecting critical infrastructure from electro-magnetic pulses.

Quantum computing:

With quantum-powered simulations, strategists can envision and optimise complex battle scenarios, leading to unprecedented precision in mission planning. When fully operational, quantum computers promise to decode encrypted enemy communications in mere seconds.

This technology may even unlock the secrets of previously unsolvable scientific challenges, leading to ground-breaking advancements in weaponry, propulsion systems and defence mechanisms.

Autonomous systems:

Accelerated AI can power autonomous vehicles, drones and robots capable of performing a wide range of tasks, from surveillance and reconnaissance to logistics and even combat operations.

5G and next-generation connectivity:

The deployment of 5G and future generations of wireless connectivity can greatly enhance military communication, data transmission and real-time collaboration. These technologies offer low latency, high bandwidth and the ability to connect a vast array of devices and sensors across the battlefield, enabling more effective coordination and the use of autonomous systems. For example, letting emergency services across the EU coordinate disaster relief efforts in real-time, just like multinational companies manage complex supply chains.

Satellite communication:

The use of satellite communication is vital for secure and reliable data transmission, particularly in remote or contested regions. Enhancing satellite communication security and resilience is essential to ensure uninterrupted connectivity for European defence operations.

Cloud computing:

A large network of data centres enabling seamless communication across land, sea, air, space and cyberspace. It integrates data, sensors and personnel for real-time decision-making, using advanced technologies like AI and cloud computing.

By consolidating information and enhancing situational awareness, it facilitates synchronised operations, enabling military forces to respond rapidly and effectively to emerging threats across diverse environments.

Digital twins and additive manufacturing:

Digital twins, virtual replicas of equipment, allow for rapid weapon prototyping and AI-powered design optimization. This, combined with predictive maintenance capabilities, ensures peak operational readiness. Meanwhile, 3D printing disrupts traditional supply chains by enabling on-demand creation of parts and even weapons directly in the field.

This reduces reliance on stockpiles and streamlines logistics, keeping forces agile in the face of evolving threats. This technological marriage promises a future of unprecedented speed, efficiency and preparedness for military operations.

Biotech:

Biotechnology is transforming defence across multiple fronts. Bioengineered materials are being developed for enhanced soldier protection and endurance. Biosensors and biodetection tools are being created for faster and more precise threat identification.

Medical advancements utilising biotechnology are leading to more effective battlefield treatments and bio-protective measures against potential biological weapons.

Energy, hypersonics and propulsion:

New, high-density energy sources like compact nuclear reactors or advanced biofuels are extending the range and operational endurance of military platforms. Hypersonic technology, with its ability to travel at extreme speeds, is redefining strike capabilities.

Advancements in propulsion systems, like hypersonic scramjets or high-efficiency electric motors, are further enhancing speed, manoeuvrability and stealth capabilities. These combined advancements are blurring the lines between conventional and strategic warfare.

Edge computing:

Computing power nearer military users can help armed forces analyse information in record time. For example, with this capability, naval forces can analyse images from underwater to conduct stealthy reconnaissance and surveillance missions with enhanced precision, tracking enemy vessels and monitoring potential threats with unmatched clarity. Ukraine doesn't have large command groups, it has smaller groups – with data on the edge, they can analyse data in real-time.

Chapter 3: Recommendations for the digital transformation of EU defence

Digital technologies are a force multiplier that can take defence capabilities to the next level. Information and data are key strategic assets affecting EU security and sovereignty. The impact of digital technologies at strategic and operational level will require close transatlantic cooperation at NATO level and support to the European digital defence industry at EU and Member State level to develop EU responses to the challenges of European armed forces.

Several obstacles stand in the way of the digital transformation of defence in Europe. They are institutional, cultural, technical and political. We have a unique opportunity to drive change now, to unite EU capabilities and become a stronger defence partner in the NATO alliance.

Collective investment strategy for the digitalisation of EU defence

The challenges we face demand a truly European response. We can and must do more. A 25% allocation for digital across EU and NATO funds, as advocated in our manifesto, is a step in the right direction.

The EU needs a common understanding of the role of new technologies. There are efforts underway to bridge this digital divide. The European Defence Agency (EDA) funds and coordinates projects across various domains, including cyber defence, artificial intelligence, and command-and-control systems. However, progress is slow due to national interests and bureaucratic hurdles.

Whilst export controls and investment screening play a role in safeguarding the EU's interests, relying solely on these reactive measures is akin to shutting the barn door after the horse has bolted. By the time investigations are complete, valuable IP may have already been misappropriated.
To truly protect our technological edge, we need a proactive approach that incentivises collaboration with friendly companies. These incentives could take the form of direct buyouts for critical technologies, strategic partnerships for joint development, or lucrative licensing agreements. By presenting a clear win-win scenario, we create a compelling reason for companies to choose collaboration over potential misappropriation.

Additionally, tax deduction schemes coordinated at EU level would be important to stimulate the development of critical digital technologies within the EU. Companies participating in collaborative projects focused on digital technology development, partnering with other private companies, universities or research institutions, should be eligible for significant tax deductions, reducing the financial burden associated with R&D in this strategic area.

25% of EU and NATO funds should be spent on digital

A true EU single market for digital

In the digital era where many technological capabilities are held within the private sector, Europe needs to build a structured public-private collaboration to strengthen resilience, and build a tech ecosystem on security and defence.

Digital needs speed and scale to succeed, and Member States' national markets are too small for technological leadership. Fragmentation creates a critical disadvantage compared to the US, which leverages a unified market to rely on just over 30 standardised systems. In contrast, Europe boasts over 170 different systems due to national preferences and exemptions.[8] This splintered approach results in smaller production runs, significantly higher unit costs and a diffusion of resources dedicated to R&D. This especially hurts our SMEs, as well as our European dual-use champions whose market potential is restricted.

To boost faster R&D and deployment of digital technologies, EU-scale procurement is a must. Whilst Member States collectively dedicate a significant portion of their budgets to defence procurement, exceeding €240 billion, the highly nationalised nature of these procurement schemes is a major roadblock.

Europe needs a system of EU-wide procurement for digital technologies allowing companies to sell to multiple countries and scale their product across borders. The recent adoption of the European Defence Industry Reinforcement Programme through common Procurement Act (EDIRPA) is a landmark achievement for EU defence cooperation.[9] It acknowledges the limitations of isolated national procurement and ushers in a new era of collaboration and efficiency. However, more needs to be done to fully realise the potential of a unified EU defence industry beyond partial reimbursement for joint procurements.

Programmes and initiatives such as the European Defence Fund (EDF), the European Defence Industrial Strategy (EDIS) and the European Defence Investment Programme (EDIP) are promising steps in the right direction to develop the EU's defence technological and industrial base (EDTIB). The EU needs to continue to bolster its digital defence sector to provide high-end, EU-made solutions for critical missions. More ambitious financial envelopes for these EU programmes would allow accompanying the digital defence industry from the research phase to commercialisation and eventual joint procurement of European-made capabilities.

[8] See Wilfried Martens Centre for European Studies, The 7Ds – Defence in Depth, available at https://www.martenscentre.eu/wp-content/uploads/2024/03/7Ds-In-Depth-Defence.pdf.
[9] Regulation (EU) 2023/2418.

Interoperability

Fragmented digitalisation levels, certifications and standards across Member States create interoperability issues. Seamless collaboration requires common standards for software and hardware, ensuring everyone operates within the same framework when in crisis or war situations, and close coordination between EU Member States and non-EU NATO allies is vital in our common fight for democracy.

Whilst some sharing occurs between the UK and Scandinavian countries, there is a noticeable lack of cooperation amongst European nations. This leads to disjointed efforts and unnecessary duplication.

There are significant variations in Member States' technological capabilities. Achieving standardisation, particularly in network interoperability, is a critical concern.

Whilst there are efforts to promote interoperability and harmonisation of standards between EU and NATO members, challenges remain due to differences in national regulations, procurement processes and industrial capabilities.

We recommend expanding the scope of the Commission's High-Level Forum on European Standardisation in the next mandate to address the challenge of disparate standards currently hindering seamless collaboration in dual-use technologies. By fostering regular dialogue and collaboration on standards, convergence between EU and NATO standards can be stimulated, streamlining procurement processes and paving the way for truly unified EU defence capabilities.

Chapter 4:
Lessons learnt from Ukraine

Ukraine's journey since 2014 can help navigate the complexities of modern warfare. Ukraine has managed to shorten its innovation adoption cycle for transformative technologies, outpacing many Western counterparts. Its military has demonstrated a willingness to embrace innovation rapidly, ensuring that emerging technologies are swiftly incorporated into operational frameworks.

Lessons of 2014

Ukraine has undergone an extensive transformation of its military over the past several years, with a fundamental overhaul of organisational structures, training methodologies and the integration of cutting-edge technologies. Emphasising the importance of adaptability, the Ukrainian Armed Forces (UAF) sought to address the changing nature of warfare and the need for rapid response capabilities. International collaboration played a pivotal role in this transformation, with partnerships fostering knowledge exchange, joint exercises and access to advanced military technologies.

The developments in Ukraine demonstrate the potential for digital solutions to tip the balance on the battlefield. Several factors aided Ukraine in navigating data-driven warfare:

Engagement of the private sector:
The Ukrainian government looked to the private sector for solutions even before Russia's full-scale invasion began.

Integration of dual-use tech:
Ukraine has used civilian commercial technologies is an integral component of defensive war.

An IT-savvy defence force and digitally literate society:
Ukrainians with IT skills became embedded in the armed forces. An educated and digitally literate population was ready to embrace the digitisation of the battlefield and contribute through the savvy use of mobile apps and other tech.

A true EU single market for digital

More than 19.2 million Ukrainians use the Diia government app, which was developed during the war and is installed on approximately 70% of smartphones in the country. Diia is often the only way for Ukrainians to receive assistance or access services provided by the Ukrainian government.

To counter Russia's regular attacks on Ukraine's digital infrastructure (targeting government data centres, mobile towers, etc.) amendments were made to Ukrainian data protection laws, enabling the government to process data in overseas cloud servers, enabling the secure transfer of critical government data.

The pivotal role of the private sector

Collaboration with the private sector has been a cornerstone of Ukraine's defence transformation. Partnerships with leading companies in defence technology, cybersecurity and ICT have allowed the military to harness the latest innovations. Flexible frameworks for engagement with the private sector have fostered an environment of continued improvement and innovation.

BRAVE1

FAST PROCUREMENT SUPPORT FOR DEVELOPMENT AND INNOVATION

Brave1 was founded thanks to the close cooperation of six key state decision-makers in the sphere of security and defence across several ministries.

It aims to speed up the development of Ukraine's defence tech ecosystem and accelerate the growth and delivery of ready-made equipment samples to the frontline. To do so, the General Staff of the Armed Forces of Ukraine prioritised 12 verticals of defence tech, including unmanned aerial and ground vehicles (UAVs and UGVs), naval drones, electronic warfare, command systems, cybersecurity, MedTech and demining.

Brave1 is aimed at defence tech innovators at any level of product/service readiness and offers a fast-track to deployment thanks to organisational support (military and business expertise, scaling and legal), information and community-building (pitches, hackathons and meetups) and finance (grants and investments).

DIGITALEUROPE represents the voice of digitally transforming industries in Europe. We stand for a regulatory environment that enables businesses to grow and citizens to prosper from the use of digital technologies.

We wish Europe to develop, attract and sustain the world's best digital talents and technology companies.

www.digitaleurope.org

@DIGITALEUROPE

DIGITALEUROPE

DIGITALEUROPE
Rue de la Science, 37
B-1040 Brussels
Info@digitaleurope.org
+32 2 609 53 10