



10 November 2025

Input to European Defence Industry Transformation Roadmap

Executive summary

Europe's defence transformation must be digital-by-design. Lessons from the war in Ukraine have shown that whilst traditional platforms remain indispensable, operational superiority now depends on the intelligent integration of digital and dual-use technologies. Artificial intelligence, autonomous systems, secure connectivity, real-time data fusion and resilient cyber infrastructure are already defining the effectiveness, responsiveness and speed of modern defence operations.

At its meeting on 23 October 2025, the European Council invited the European Commission to present a roadmap for transforming the defence industry — a critical opportunity to strengthen Europe's technological and industrial base and bridge the gap between digital innovation and defence readiness.

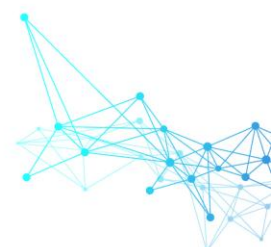
[DIGITALEUROPE](#), representing digitally transforming industries across defence, dual-use and civilian technologies, welcomes this effort and stands ready to contribute. Building on cross-sector expertise, this paper provides industrial input to inform and support the development of the forthcoming European Defence Industry Transformation Roadmap (EDITR). It outlines the policy, funding and governance foundations necessary to establish a digitally enabled, competitive and resilient European defence ecosystem.

Europe's defence digitalisation faces long-standing barriers, including market fragmentation, regulatory inconsistency and limited interoperability. Overcoming these barriers requires a coherent and forward-looking approach that embeds digital and dual-use technologies from the earliest stages of capability planning and procurement. This transformation should be guided by capability requirements and operational priorities, whilst remaining digitally driven, industry-inclusive and human-centred. It should also leverage commercial innovation and proven solutions from qualified providers within the EU and trusted international partners, demonstrating how dual-use technologies strengthen both economic competitiveness and defence readiness.

Building on this ambition, DIGITALEUROPE proposes the [Copenhagen Project](#), a pan-European framework to channel European Union (EU) resources, combined with national budgets, to rapidly deploy dual-use digital technologies that protect critical infrastructure, enhance resilience, and build Europe's next generation of digital champions.

To achieve the above, DIGITALEUROPE calls on the forthcoming EDITR to:

- ▶▶ **Integrate defence and dual-use digital technologies** from the earliest stages of capability planning and procurement;
- ▶▶ **Establish a secure and interoperable digital backbone** for connectivity, data, cloud, quantum communications and AI-enabled systems across all operational domains;
- ▶▶ **Empower innovators and solution providers across the industrial spectrum**, from large enterprises to SMEs and start-ups, as full participants in Europe's defence modernisation;



- ▶▶ **Harmonise standards and regulatory frameworks** to enable cross-border cooperation and interoperability; and
- ▶▶ **Invest in the digital skills and mobility** essential for a competitive, digitally-enabled and resilient defence sector.

DIGITALEUROPE identifies **seven key enablers** that together can translate Europe's digital ambition into operational capability and sustained defence transformation (see Figure 1). Together, these enablers outline the key steps to modernise Europe's defence ecosystem and form the foundation of a secure, agile and technologically resilient European defence industry.

Figure 1. DIGITALEUROPE's Seven Key Enablers for Europe's Defence Technological Transformation



Table of contents

Executive summary	1
Table of contents	3
Seven key enablers for accelerating Europe's defence transformation	3
I. Digital-by-design defence transformation.....	3
II. Secure and interoperable defence digital network.....	4
III. Agile defence innovation ecosystem	5
IV. Regulatory and standards coherence for defence digital transformation.....	6
V. Testing, validation and certification network	7
VI. Scaling innovation: from lab to deployment	8
VII. Skills and mobility for digital defence.....	9
Conclusion	10

Seven key enablers for accelerating Europe's defence transformation


I. Digital-by-design defence transformation

Barrier: Digital technologies, including trusted and secure advanced connectivity, AI, cybersecurity, cloud, quantum, and data analytics, are still often integrated late in capability programmes.

Why it matters: Embedding digitalisation from the outset is essential for modern civil and military readiness. When systems are designed digitally from inception, they become more adaptable, interoperable and secure.

Proposed solutions:

- ▶▶ **Systematically embed digital-by-design principles** across EU and national defence planning frameworks, treating digital technologies as strategic enablers rather than optional add-ons.
- ▶▶ **Allocate a meaningful share of new EU and national defence investments**, for example, around **25%**, to digital and dual-use technologies, including secure and interoperable advanced connectivity, AI, cyber, quantum and data, across the defence planning and capability lifecycle. This should draw on qualified providers within the EU and trusted international partners, whilst strengthening Europe's industrial and technological base.
- ▶▶ **Publish reference digital architectures and technical guidance** for interoperability and system integration, co-designed with Member States and industry, to serve as a voluntary framework to align national and EU programmes.

- 
- ▶▶ **Define clear digital performance criteria and measurable innovation indicators** in capability planning, R&D and procurement (e.g. interoperability benchmarks, cybersecurity assurance levels, digital readiness indicators) to track and reward progress.
 - ▶▶ **Leverage insights from European Defence Fund (EDF)-supported capability projects**, particularly those initiated or co-sponsored by Ministries of Defence (e.g. through Letters of Intent), to inform and accelerate Europe's digital transformation and information-superiority objectives.
 - ▶▶ **Plan early for the replacement of end-of-life and unsupported systems** to reduce technical debt, improve cybersecurity and ensure seamless integration with digitally designed capabilities.

Expected outcome:


- ▶▶ **By 2028, digital-by-design principles** are systematically embedded in new capability programmes and mainstreamed across EU and national defence planning and funding instruments.
- ▶▶ **Early adoption of digital-by-design approaches** delivers cross-border benefits, enabling faster deployment of interoperable, information-superiority capabilities.
- ▶▶ **Lifecycle costs reduced** through early digital integration (for instance, by 30%).
- ▶▶ **Common digital standards and architectures** enable real-time data exchange and multi-domain interoperability across European and partner systems.
- ▶▶ **Defence procurement fosters** a culture of innovation and faster technology transfer between civil and military domains.

II. Secure and interoperable defence digital network

Barrier: Europe's defence digital landscape remains fragmented. National systems for secure communications, data management and cloud hosting follow differing standards and accreditation schemes, limiting interoperability, slowing crisis response and preventing Europe from operating as a cohesive, data-driven defence ecosystem.

Why it matters: Modern defence operations rely on fast, interoperable and secure data sharing across domains and borders. Establishing a common foundation for interoperability without centralisation will enable Member States, partners and industry to work together effectively whilst preserving sovereignty and security.

Proposed solutions:

- ▶▶ **Adopt a secure and interoperable defence connectivity backbone** based on shared and recognised standards (such as 5G, aligned whenever relevant with NATO interoperability frameworks). This backbone should enable the interconnection of national and European secure cloud and communication platforms, open to qualified providers from the EU and trusted international partners.
 - ▶▶ **Promote hybrid and multi-cloud deployment models** to enhance assurance, resilience and interoperability across defence digital infrastructures, building on cybersecurity and accreditation frameworks.
- 

- 
- ▶▶ **Develop a federated European Defence Data Space**, building on this connectivity backbone, to enable secure, cross-border data exchange and operational data use across Member States, whilst ensuring national data sovereignty. This Data Space should leverage existing trusted data-sharing frameworks and recognised security standards.
 - ▶▶ **Make interoperability and cybersecurity baseline criteria** in defence funding and procurement, ensuring consistency from research to deployment.
 - ▶▶ **Foster public–private collaboration** to develop modular reference architectures and data-exchange models supporting both defence and civil-security missions.
 - ▶▶ **Promote alignment between European and NATO technical standards**, taking into account NATO's digital transformation strategy and digital backbone reference architecture, to ensure interoperability and prevent duplication across joint operations.

Expected outcome:

- ▶▶ **By 2030**, all new major EU and national defence digital systems and progressively existing ones, operate within a secure and interoperable network.
- ▶▶ **Trusted data exchange** enables real-time coordination and joint situational awareness through an interoperable digital connectivity backbone.
- ▶▶ **Reduced duplication and greater resilience** through shared standards and modular architectures.
- ▶▶ **Modern, interoperable Command and Control (C2) platforms** enable combined and multidomain operations, turning Europe's growing data landscape into a strategic advantage.
- ▶▶ **A connected and data-driven defence ecosystem** that strengthens Europe's resilience and global competitiveness.


III. Agile defence innovation ecosystem

Barrier: Defence innovation in Europe remains slowed by complex procedures, fragmented demand and lengthy procurement cycles. Dual-use providers, SMEs and start-ups often face restrictive eligibility criteria and heavy administrative burdens. As a result, many promising civilian technologies fail to transition into operational defence use.

Why it matters: Europe's security and competitiveness depend on mobilising innovation across its entire industrial base. Enabling the full participation of the dual-use ecosystem accelerates the adoption of emerging technologies, including secure connectivity, AI, cybersecurity, quantum, robotics, and space, thereby strengthening Europe's technological resilience. This is particularly evident in cybersecurity, where protecting critical infrastructure such as ports, hospitals and energy facilities enhances both civil and defence resilience. Supporting dual-use cyber capabilities through EU instruments, such as the EDF and the EU Defence Innovation Scheme (EUDIS), can help fast-track pilot projects and demonstrate the value of agile innovation models.

Proposed solutions:

- ▶▶ **Establish a single-entry innovation gateway at the EU level** that integrates outcome-based, dynamic and agile procurement pathways, enabling public authorities and industry, including large



enterprises, midcaps, SMEs and start-ups, to co-develop, test and contract innovative solutions through simplified, performance-driven processes.

- ▶▶ **Strengthen coherence between defence and digital innovation programmes**, linking the EDF and EUDIS with wider EU instruments to streamline access and avoid duplication.
- ▶▶ **Encourage early public-private co-investment** by de-risking initial phases, clarifying regulatory frameworks and enabling faster market entry for emerging technologies.
- ▶▶ **Enhance strategic prioritisation of defence investments** to align R&D with capability needs, building on the European Defence Agency's (EDA) Overarching Strategic Research Agenda (OSRA).
- ▶▶ **Promote regional innovation clusters and cross-border cooperation**, expanding participation beyond major capitals through targeted outreach and funding.
- ▶▶ **Integrate a dedicated innovation track** within major European defence events to connect end-users, investors and innovators around practical capability challenges.

Expected outcome:


- ▶▶ **Broader participation of dual-use innovators in EU-funded defence R&D**, with SMEs and start-ups increasing their share from **42 to 50%** of participants and from **18 to 25%** of total funding by 2030, strengthening Europe's innovation capacity.
- ▶▶ **Procurement and validation cycles shortened by around 40% by 2030** compared with 2024 levels, accelerating the deployment of emerging technologies and strengthening Europe's capacity for rapid adaptation.
- ▶▶ **Enhanced cross-sector collaboration and faster technology transfer** between civil and defence ecosystems, improving Europe's ability to scale dual-use solutions.
- ▶▶ **A more inclusive, competitive and innovation-driven European defence ecosystem**, built on public-private cooperation, shared technological ambition and measurable progress tracked through existing EDF and EUDIS indicators.

IV. Regulatory and standards coherence for defence digital transformation

Barrier: Fragmented national rules on data classification, cloud accreditation and facility clearance create duplication, higher costs and delays. The absence of mutual recognition prevents efficient cross-border cooperation, particularly disadvantaging the dual-use innovation ecosystem.

Why it matters: Without secure and interoperable regulatory frameworks, technologies validated in one Member State cannot be easily deployed in another. Achieving coherence requires interoperability, not uniformity; it is the foundation for speed, trust and competitiveness in Europe's defence transformation.

Proposed solutions:

- ▶▶ **Strengthen governance and coordination** for dual-use digital technologies by promoting coherent criteria and closer cooperation between EU and national programmes, reducing fragmentation and overlap.
- 

- ▶▶ **Introduce mutual-recognition mechanisms** for facility, personnel and digital-security certifications where equivalent protection standards apply, reducing repetitive audits and re-authorisations. These mechanisms should align, where relevant, with NATO and other internationally recognised security certification processes.
- ▶▶ **Develop common guidance for RESTRICTED-level data handling and cloud security**, offering reference criteria and documentation templates for national adoption and alignment with NATO practices where appropriate to ensure interoperability.

Expected outcome:

- ▶▶ **Faster authorisation and deployment** of digital and dual-use systems through reduced duplication and clearer procedures.
- ▶▶ **Lower administrative burden** and greater participation of the dual-use innovation ecosystem, supported by predictable and transparent compliance requirements.
- ▶▶ **A coherent, trusted regulatory environment** that facilitates cross-border cooperation and accelerates Europe's defence digitalisation.

V. Testing, validation and certification network

Barrier: Europe lacks a coordinated network for testing and validating digital and dual-use defence technologies. Existing facilities operate in isolation, applying different standards and methodologies. This fragmentation limits trust, delays certification and hinders technology transfer across Member States.

Why it matters: Fast and trusted validation is essential for operational deployment. Without interoperable testing and certification processes, innovative solutions often face delays of months or even years before being deployed in the field. A coordinated European framework would shorten time-to-deployment, enhance mutual trust among Member States and give industry a competitive edge in global markets.

Proposed solutions:

- ▶▶ **Develop a coordinated European framework**, linking national and industrial testing facilities through standard protocols, transparent audit criteria and alignment with EDA's initiatives, including the Defence Test and Evaluation Base (DTEB), IT Platforms and the Hub for Defence Innovation (HEDI), notably its **Operational Experimentation** (OPEX).
- ▶▶ **Establish shared EU-level cybersecurity testbeds** to assess both military-grade and dual-use solutions in controlled environments, including those for AI-enabled cyber-defence applications.
- ▶▶ **Promote mutual recognition of testing and certification results** where equivalent assurance standards apply, reducing duplication, costs and delays.
- ▶▶ **Encourage coordination with NATO and other trusted international frameworks** to ensure complementarity, avoid duplication and strengthen cross-alliance interoperability.
- ▶▶ **Integrate “test-before-invest” mechanisms** into EU defence programmes (EDF, EUDIS) to accelerate validation and deployment of emerging technologies.
- ▶▶ **Encourage alignment of civilian and defence certification schemes** (e.g. in cyber, cloud, AI) to support dual-use innovation and interoperability.

Expected outcome:

- ▶▶ **Shorter validation cycles** and faster transition from demonstration to operational deployment.
- ▶▶ **Increased trust and interoperability** through shared testing protocols and recognised certifications.
- ▶▶ **Lower cost and administrative burden**, enabling broader participation of the dual-use innovation ecosystem in the defence value chain.
- ▶▶ **A credible and connected European testing and certification network** that enhances readiness, market access and industrial competitiveness.

VI. Scaling innovation: from lab to deployment

Barrier: Europe continues to face delays in translating promising research and prototypes into deployable defence capabilities. Fragmented procurement, a lack of continuity in funding after pilots, and weak coordination between research, testing, and operational adoption hinder the scaling of innovations, particularly for SMEs and dual-use providers.

Why it matters: Bridging the gap between innovation and deployment is crucial for readiness and competitiveness. Without predictable scaling mechanisms, validated technologies often remain stuck at the prototype stage, wasting public investment and discouraging private co-investment. A coherent deployment methodology would ensure that innovations proven in testing environments are fielded rapidly, securely and at scale.

Proposed solutions:

- ▶▶ **Establish pre-allocated post-pilot funding streams and a fast-track mechanism** within EU defence programmes to ensure continuity from validation to deployment, enabling technology delivery at the pace required for operational relevance.
- ▶▶ **Adopt phased, outcome-based and capability-driven contracting** that rewards performance, adaptability and interoperability whilst reducing deployment risk, supporting the adoption of certified, high-performing solutions that strengthen operational readiness.
- ▶▶ **Create a Deployment Readiness Framework** to assess interoperability, scalability and cybersecurity of emerging technologies prior to adoption, complemented by an EU-level *use-case library* documenting validated dual-use applications, benefits and lessons learned to support replication.
- ▶▶ **Foster early-adopter partnerships (anchor-customer models)** between ministries, industry and SMEs to accelerate initial deployments and create confidence for wider uptake.

Expected outcome:

- ▶▶ **Faster transition from innovation to capability**, overcoming the “valley of death” through joint experimentation and predictable scaling mechanisms.
- ▶▶ **Shorter transition timelines** from prototype to operational capability, enhancing readiness and responsiveness.

- ▶▶ **Increased private-sector investment confidence** supported by transparent, results-oriented deployment processes.
- ▶▶ **Stronger industrial credibility** and competitiveness through measurable deployment standards and demonstrated operational impact.

VII. Skills and mobility for digital defence

Barrier: Europe faces a growing shortage of professionals with advanced digital skills relevant to defence. Fragmented training systems, differing clearance requirements and limited mobility across sectors prevent industry and governments from accessing the expertise needed to deploy and secure emerging technologies.

Why it matters: Digital transformation in defence depends on human capacity. Without qualified professionals in cybersecurity, AI, data and cloud, technological investments cannot translate into operational readiness or resilience.

Proposed solutions:

- ▶▶ **Establish structured partnerships** between industry, academia and defence organisations, leveraging and scaling successful industry-led training initiatives, to co-develop programmes in cyber, data, AI and secure software engineering that strengthen cooperation between public and private stakeholders.
- ▶▶ **Promote mutual recognition** of security clearances and professional credentials in digital domains to facilitate workforce mobility and project participation, whilst respecting national prerogatives.
- ▶▶ **Integrate defence-related modules** into existing EU digital-skills programmes to bridge civil–military knowledge gaps and create clearer career pathways.
- ▶▶ **Strengthen cooperation between the European Security and Defence College (ESDC)** and the defence-industrial ecosystem to incorporate industrial insights into digital and cybersecurity modules and, where relevant, open training to industry participants to foster a shared defence and security culture.
- ▶▶ **Align training and certification frameworks** with the EU Pact for Skills and the Digital Skills & Jobs Platform, ensuring coherence and scalability across Europe.

Expected outcome:

- ▶▶ **A stronger and interoperable pool of digital professionals** able to work across sectors and borders.
- ▶▶ **Shorter recruitment and onboarding timelines** for defence-related digital roles.
- ▶▶ **Improved retention and continuous upskilling of digital professionals** through sustainable training pathways and lifelong learning mechanisms.
- ▶▶ **A coordinated European training and certification ecosystem** ensuring consistency, mutual recognition and long-term talent development.

- ▶▶ **Stronger civil–military–industrial cooperation** in digital skills development, fostering a shared European defence and security culture.
- ▶▶ A **skilled, mobile and trusted workforce** supporting innovation, resilience and operational effectiveness.

Conclusion

Whilst major national and EU initiatives have advanced Europe's defence innovation agenda, they have not yet placed sufficient emphasis on the digitalisation of defence capabilities and the opportunities it creates. Embedding digital transformation at the design stage of every future capability is essential to ensure readiness, resilience and technological leadership. At the core of Europe's Defence Industry Transformation lies the need for a unified mechanism that connects innovation with deployment, digitalisation with resilience, and industry with citizens' protection.

The *Copenhagen Project*, initiated by DIGITALEUROPE, builds on the Danish model that helped Ukraine by funding its defence industry and rapidly delivering capabilities. Adopted by the EU and partners as an effective government–industry mechanism, it showed how resources can be channelled efficiently. Extending this model to civil and dual-use domains, the *Copenhagen Project* aligns EU and national instruments — including unspent funds, new EIB models, EU-level joint procurement, and the forthcoming Competitiveness Fund — to accelerate deployment of advanced digital technologies. It will protect critical infrastructure and citizens through cyber-secure, energy-resilient systems; boost scalable digital investment under a unified EU–national framework; and restore Europe's global competitiveness by fostering new digital champions across civil, dual-use, and defence domains. Turning Europe's digital ambition into a tangible “Digital Shield,” the *Copenhagen Project* brings the Roadmap's vision to life.

The **seven enablers** outlined in this paper, spanning digital integration, interoperability, innovation, regulation, validation, scaling and skills, **offer a practical roadmap** toward a more agile and competitive European defence ecosystem. The forthcoming **Roadmap** presents a decisive opportunity to deliver this transformation by translating these enablers into a concrete **Action Plan** with clear priorities, responsibilities, and timelines. **DIGITALEUROPE** recommends that this **Plan** focus on **five immediate priorities**:

- ▶▶ **Embedding digital-by-design principles** in all new capability programmes.
- ▶▶ **Developing a secure and interoperable digital defence backbone** for data and communications.
- ▶▶ **Establishing a coordinated European network** for testing and validating dual-use digital technologies.
- ▶▶ **Reinforcing cyber resilience** across all digitised systems and platforms.
- ▶▶ **Investing in digital skills and innovation ecosystems** to enable cross-border collaboration and faster technology scaling.

The implementation of this plan should be supported by a **dedicated governance mechanism** that ensures transparency, accountability and continuity through measurable indicators and regular progress reviews. **DIGITALEUROPE** remains committed to working with the **European Commission**, the **European Defence Agency** and **Member States** to ensure that this transformation is **digital-by-design, innovation-driven and future-ready**.



FOR MORE INFORMATION, PLEASE CONTACT:

Dr Constantinos Hadjisavvas

Director, Digital Resilience and Defence

constantinos.hadjisavvas@digitaleurope.org

Neus Rodriguez

Manager for Defence and Strategic Connectivity

neus.rodriguez@digitaleurope.org

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory and investment environment that enables European businesses across multiple sectors, as well as citizens, to prosper through digital technologies. We wish Europe to grow, attract and sustain the world's best digital talent, investment and technology companies. Together with our members, we shape industry positions on all relevant policy matters and contribute to their development and implementation. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations and scaleups which are global leaders in their fields, as well as national trade associations from more than 30 European countries.

