The world is how we shape it

sopra steria

A new model for European tech innovation

Sopra Steria's contribution to the EU defence transformation roadmap

The European Commission's EU Defence transformation roadmap represents a timely and strategic opportunity to promote the integration of new technologies into defence from the outset. As a leading European digital company in the defence sector, we believe that the current model to develop and integrate new technologies must be better adapted to the specific demands of the digital age.

— This position paper outlines Sopra Steria's recommendations for a new model of European defence innovation and modernisation, built on speed, sovereignty, and strategic enablers.

Summary

01

The need to adapt the defence innovation model to the digital age

Sopra Steria believes that the current model for fostering innovation suffers from a fundamental «hardware bias» that is ill-suited to the speed, complexity, and strategic imperatives of digital technologies. This approach leads to three critical issues:

A. The time to operational deliver.

The current **defence innovation system is too slow for software development.** The longer cycles of the European Defence Fund **(EDF) do not fit adequately with the pace of digital innovation.** The current model guarantees that by the time a European digital solution is delivered through the EDF, it is already at risk of being obsolete or dominated by non-EU players.

B. Fragemented governance of digital dual-use tech

Governance in digital technologies is spread across a fragmented landscape of EU (DG DEFIS, DG CNECT, EDA, etc.) and national authorities in both the digital and defence sectors. As a result, **funding is scattered across various instruments** (EDF, EIC, Horizon Europe, DigitalEurope...), **each with different eligibility rules and without unified governance.** This creates a lack of visibility on available opportunities and requires significant effort to navigate varied administrative requirements. More importantly, **this budget fragmentation hinders the development of large-scale projects** that would deliver the strategic and sovereign dual-use digital capabilities Europe needs.

C. Aligning innovation with operational needs

While research and technological development naturally involve a degree of exploration and uncertainty, innovation intended for defence should remain closely connected to operational realities. Projects developed in isolation from end-users risk failing to address real needs or gaining traction among those who will ultimately rely on them. The lesson from Ukraine is clear: **rapid innovation is only effective when it involves a short, direct feedback loop with the end-user.**

02

Sovereignty by design as a foundational pillar

« Digital technologies are among the areas where Europe faces its most critical strategic dependencies. »

As the backbone of modern systems, digital infrastructure is inherently tied to our ability to act autonomously. These dependencies therefore present major risks to our sovereignty, particularly in the defence domain. To address this challenge, Europe must act on two key fronts: industrial sovereignty and digital sovereignty.

A. Industrial sovereignty: A European preference in dual-Use funding

The diverging eligibility criteria in different EU funds for digital and dual-use technologies poses systemic risks that should be prevented. **We propose establishing a single, unified eligibility standard for all EU-funded dual-use projects, using the EDF criteria as the baseline.**

B. Digital sovereignty: Cybersecurity by design

Sovereignty is not only about where a technology is built, but how it is built. Cybersecurity must be treated as a foundational element, designed and embedded into digital defence systems from the outset.

Any new digital infrastructure for defence funded by the EU must be built on solid cybersecurity principles. This includes:

- **Zero Trust Architecture (ZTA):** Moving beyond the traditional «secure perimeter» model, ZTA requires continuous verification of every user, device, and connection, ensuring that even if an attacker gains access, lateral movement is restricted.
- **Data-Centric Security (DCS):** Shifting the focus from protecting the «container» (e.g., network or device) to protecting the «content» (the data itself). With DCS, each piece of

information is encrypted and protected individually, so even if a system is breached, the data remains useless to adversaries.

In addition, **cybersecurity certifications for digital technologies,** such as cloud, AI, and quantum, **should address both technical and non-technical risks** (i.e. supply chain integrity, legal and governance risks, or geopolitical exposure). These certifications would help establish a common baseline for cybersecurity and sovereignty in dual-use systems.

« Finally, the EU's cybersecurity doctrine must be future-proof, including a clear roadmap for the migration to Post-Quantum Cryptography (PQC) to safeguard against next-generation threats. »

03

The pillars of the transformation

« We propose that the Defence transformation roadmap's approach takes into account four foundational pillars: a new governance to accelerate defence innovation, a digital backbone working as a force enabler, modern command and control platforms for combined, multidomain operations, and a use-case driven approach in technology. »

A. A fast-track innovation governance

A fast-track innovation governance could take the form of a permanent, open call within the EDF. This mechanism could be built on three core principles:

- **Short cycles (18-24 months):** The process from project submission to project delivery should be radically shortened. We propose a six-month window for funding decisions and an 18-month target for project implementation, ensuring technology is delivered at the speed of relevance.
- **An operational loop with end-users:** Innovation must be driven by operational needs. We propose a direct, short-cycle testing and feedback loop with armed forces for every funded project at TRL 3 or above. This moves technology out of the lab and ensures that what we build provides tangible value to the end-user.
- **Unified governance:** To overcome the fragmentation of dual-use governance, this fast-track mechanism should have a single, designated pilot. The European Commission should empower one of its entities to coordinate these innovation projects across the relevant Commission DGs, ensuring strategic coherence and efficiency.

B. Building the digital backbone for European defence

Data is the fuel for innovation, the foundation of trustworthy AI, and a key enabler for

achieving decision superiority on the modern battlefield. Europe possesses vast reserves of high-quality data across its member states. Yet, this strategic asset remains untapped, fragmented and locked away in national and sectoral silos, inaccessible due to a lack of trust, common standards, and secure interoperability frameworks. This fragmentation is a major brake on our defence transformation.

« The solution is not to centralise this data. The solution is to federate it through a single, unifying project: the European Defence Data Space. »

A Data Space is not a central database; it is a secure, common language. It is a federated ecosystem that allows national systems to interoperate while each Member State retains full sovereignty over its own data, deciding what to share, when, and with whom. This is how we build trust, digitally.

The Data Space is the foundational enabler for the disruptive capabilities Europe needs. Some key use cases include enabling a truly data-centric command and control, training sovereign AI applications for defence or powering high-fidelity simulations and digital twins for mission rehearsal, predictive operations, logistics, and maintenance.

A Defence Data Space could start with military mobility as its main use case. This Data Space would serve as the common digital backbone for European logistics, enabling the real-time exchange of data on fuel levels, ammunition stocks, spare part availability, or maintenance schedules across borders. This would immediately enhance the resilience and efficiency of any deployment. European defence funding projects such as EDF could contribute to the development of this architecture.

C. New Command and Control (C2) platforms

A successful defence transformation should enable Europe to conduct effective combined and multidomain operations. The modern battlefield is defined by a flood of data from a vast array of sensors across all domains. To turn this complexity into a strategic advantage, **Europe needs a new generation of C2 platforms able to exploit data to its fullest to support combined, multidomain operations.**

A modern C2 architecture must be able to fuse massive, diverse datasets in real-time to create a single, trusted operational picture; seamlessly integrate manned and unmanned systems, enabling true human-machine teaming; and unlock combined and joint operations in a multi-domain environment by breaking down silos. These platforms must be built on an open, modular architecture ('plug & play'), allowing for the rapid integration of new capabilities via APIs. This ensures adaptability and prevents vendor lock-in.

In essence, modern command and control platforms are the core enabler that transforms the ambition of interoperability into practical, operational reality.

D. The investment focus: A use-case-driven approach

We advocate for A use-case driven approach, mostly targeted around AI, sovereign cloud and quantum where investment is targeted at solving real-world operational problems. Particularly in three fundamental technologies, AI, sovereign cloud and quantum.

AI

This technology is set to redefine the operational and strategic landscape of the defence sector. One of the primary roles of AI in defence is to accelerate the journey from raw data to decisive action. We suggest focusing investment on two critical use cases:

- **Decision superiority:** Developing sovereign AI tools for sensor fusion, predictive analytics, and advanced simulation to provide commanders with a clear, trusted operational picture and enable faster, better-informed decisions.
- **Cognitive superiority:** Building AI-powered capabilities to counter Foreign Information Manipulation and Interference (FIMI) campaigns. As generative AI becomes a powerful threat multiplier in cognitive warfare, Europe needs to develop its own sovereign AI tools for detection, analysis, and response.

Crucially, all investment in AI for defence must be guided by an unwavering commitment to develop systems that are **trustworthy, transparent, sovereign, and human-centric.**

Europe's dependency on non-EU cloud providers in the civil domain cannot be replicated in the defence sector as this would create an unbearable strategic vulnerability. Therefore, the EU must **prioritise a clear strategy for the development of sovereign, secure, and combat-ready clouds.** This would be central to our data security, sovereignty, and the resilience of our most critical defence applications.

Sovereign cloud

Europe's dependency on non-EU cloud providers in the civil domain cannot be replicated in the defence sector as this would create an unbearable strategic vulnerability. Therefore, the EU must **prioritise a clear strategy for the development of sovereign, secure, and combat-ready clouds.** This would be central to our data security, sovereignty, and the resilience of our most critical defence applications.

Quantum

The primary barrier to adopting quantum computing is identifying use cases with real operational impact. To prepare for a quantum-enabled defence, the EU **should launch targeted programmes and pilot projects to identify, test, and validate high-impact military applications,** ensuring our R&D efforts are systematically aligned with future operational needs.

From individual capabilities to a coherent European ecosystem. To translate these use cases into a real strategic advantage, **the European defence transformation cannot focus simply on innovation, but also on building a coherent operational ecosystem.**

- ***Technology federation.*** Europe possesses pockets of world-class technological excellence across several technological domains. However, these sovereign capabilities operate in isolation, with no single provider capable of meeting the full spectrum of defence needs. We therefore propose that the EU **create a dedicated funding stream within its innovation programmes for technology federation.** The goal should be to **create integrated platforms that combine complementary, best-in-class sovereign solutions from various European providers into a single, world-class offering.**
- ***Technology integration and adoption.*** The level of digitalisation and modernisation across armed forces in Europe is uneven. A focus on disruptive innovation alone must not overshadow the urgent need for widespread technology adoption. Support for innovation must be paired with **a dedicated funding stream for technology integration. The commission should also encourage member states to make the relevant efforts to have their armies meet the standards of the Digital age.** This should fund the practical, essential work of automating and digitising procedures, deploying secure communications, and accelerating the migration of legacy systems to secure, sovereign cloud environments. This approach ensures that we are not only building the future, but also mastering the present, bringing all our forces up to a common, resilient digital standard.

Conclusion

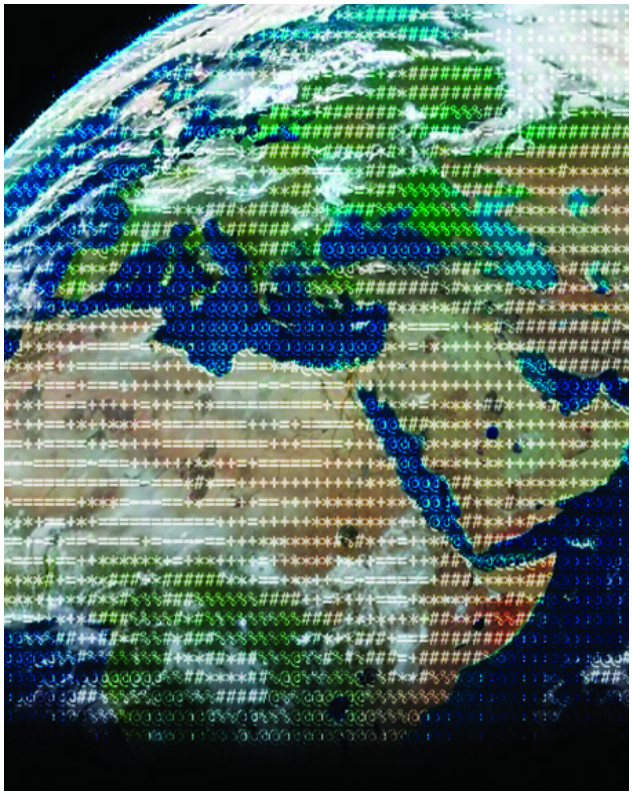
Europe stands at a critical juncture in the digital transformation of its defence sector. The ambition set by the European Commission's defence transformation roadmap is both timely and necessary. Real transformation requires a fundamental shift, not only in technologies, but also in the way we govern, invest, and collaborate.

— The European Union needs a new framework built on speed, operational relevance, digital sovereignty, and trusted partnerships with industry.

This means accelerating project timelines, embedding cybersecurity and sovereignty from the start, and aligning innovation with the real-world needs of our armed forces.

To build the capabilities that Europe's defence demands, the EU must prioritise:

- **A fast-track innovation mechanism** that matches the pace of digital development;



- **A sovereign European Defence Data Space** to unlock the value of data as a strategic asset;
- **Modern Command and Control platforms** to enable combined, multidomain operations;
- **Investment in high-impact use cases** in AI, sovereign cloud, and quantum;
- And finally, a coherent ecosystem approach that **federates our strengths** and ensures **technology adoption and digitalisation.**

The world is how we shape it

sopra steria

Sopra Steria

6 avenue Kleber
75116 Paris

+33(0)1 40 67 29 29

https://www.soprasteria.com/

https://www.linkedin.com/company/soprasteria/