THE EXECUTIVE BRIEF:

BOOSTING EUROPEAN DIGITAL DEFENCE INNOVATION

DIGITALEUROPE

Traditional defence systems alone no longer guarantee security. Today's hybrid conflicts – blurring the lines between peace and war – rely on disruptive but low-cost tools like drones, cyberattacks and misinformation. These tactics paralyse critical infrastructure, disrupt societies and erode military effectiveness.

Europe's defence capabilities are at a crossroads. Digitalisation is no longer optional—it is essential to maintaining security, countering hybrid threats, and ensuring operational superiority. Modern defence requires real-time intelligence, resilient digital infrastructure, and advanced cybersecurity to safeguard critical entities from digital attacks and electronic warfare.

Achieving these goals demands greater interoperability across EU armed forces and allies, investment in dual-use technologies —including AI, big data, quantum computing, 5G and next-generation connectivity, satellite communication, and additive manufacturing— and stronger public-private collaboration to match the speed of commercial innovation.

Europe must act now. Without swift action, it risks falling behind in an era where digital threats evolve faster than traditional defence structures can adapt.

This briefing note outlines three key messages to advance European Digital Defence Innovation, backed by six success indicators and nine policy recommendations, which are further explained in the Annex.

Three Key Messages

1

Europe's defence future depends on digitalisation – we must act now

Traditional defence structures cannot keep pace with the speed and complexity of modern hybrid threats. The EU must allocate at least 25% of new defence spending to digital and dual-use technologies to maintain security and resilience. Critical entities—power grids, communication infrastructure, hospitals, airports, water suppliers, mobility infrastructure, etc.—are highly vulnerable to digital attacks and electronic warfare. Europe must invest in AI-driven cybersecurity, quantum encryption, next-generation cloud computing, advanced sensor networks, autonomous systems, and 5G/6G connectivity to protect vital infrastructure, enhance situational awareness, and counter evolving threats.

2

A single European defence market is key for speed and scale

Fragmented national defence procurement slows innovation, drives up costs, and weakens Europe's ability to respond to crises. The EU must establish a Single Defence Market, standardise procurement, and prioritise joint investment in emerging technologies to strengthen supply chain resilience and accelerate deployment. Defence innovation cycles must match commercial technology speeds (12–24 months), not decades. A stronger focus on semiconductors, space-based intelligence, encrypted communications, digital twins, and edge computing will ensure the rapid integration of new capabilities. Modernisation, coordinated investments, and public-private collaboration are critical to driving defence resilience and equipping Europe with cutting-edge solutions.

3

Stronger defence partnerships with NATO, the US, and Ukraine

Europe's security cannot be safeguarded in isolation. The EU must enhance strategic collaboration with NATO, transatlantic allies, and Ukraine to ensure interoperability and joint technological advancements. Establishing an EU-US Dual-Use and Critical Tech Council will ensure Europe remains a leader, not a follower, in digital defence innovation. Closer EU-Ukraine cooperation is essential to modernising battlefield technology. A joint EU-Ukraine initiative could develop next-generation battlefield communication systems, enhancing real-time intelligence, secure connectivity, and interoperability across allied forces. These advancements could later be adapted for civilian use, including infrastructure protection and emergency management, further strengthening Europe's resilience.

Success Indicators:

25%
By 2030, allocate 25% of EU and Member States' new defence expenditure to digital, emerging technologies, and dual-use technologies to enhance operational readiness and resilience.

75%
By 2030, ensure that 75% of EU-funded dual-use technology projects enhance the resilience of critical infrastructure – including energy, transport, and data centres – by strengthening AI-powered cybersecurity, secure communications and defence interoperability.

3
By 2030, launch three large-scale defence and dual-use technology procurement programs, ensuring alignment with commercial innovation cycles (12-24 months) and prioritising investments that secure digital and physical infrastructure against hybrid threats. This will accelerate adoption, enhance interoperability, and strengthen supply chain resilience.

40%
By 2028, reduce defence procurement timelines by 40 per cent through digitalisation, ensuring critical technologies are delivered within 12-24 months instead of the current multi-year timeline.

>120
By 2030, the EU should reduce the number of different defence systems from 172 to approximately 120 through joint procurement, coordinated R&D, and standardisation, enhancing interoperability, cutting costs, and improving defence readiness across Member States and NATO allies.

75,000
By 2028, train and certify at least 75,000 skilled professionals in defence-related digital fields through EU and NATO funded programmes, with a dedicated focus on both new talent and the reskilling of defence personnel to meet evolving digital requirements.

9 Policy recommendations

1 Protect Critical Entities and Enable EU Resilience Through Advanced Technologies

2 Advance Digital Defence and Dual-Use Technologies

3 Address the Digital Defence Skills Gap

4 Establish a Single Defence Market for Technological Competitiveness

5 Promote Joint Procurement to Strengthen the Defence Market and Drive Innovation

6 Accelerate Production Capabilities and Resilient Supply Chains Through Earmarking Investment

7 Enhance Collaboration with Ukraine on Technologies and Innovation

8 Strengthen EU-NATO Collaboration on Digital Security and Defence Interoperability

9 Deepen EU-US Cooperation on Dual-Use and Critical Technologies

DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies.

We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies.

Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 108 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

𝕏 @DIGITALEUROPE

⬡ @digitaleurope_org

in DIGITALEUROPE

▶ @DIGITALEUROPEvideo

www.digitaleurope.org