DIGITALEUROPE

5 KEY RECOMMENDATIONS TO DELIVER DIGITAL DEFENCE READINESS BY 2030

Five recommendations.
Five concrete targets.





FIVE RECOMMENDATIONS. FIVE CONCRETE 2030 TARGETS.

These recommendations are intended to support the delivery of **Defence Readiness 2030**. They should also help inform the next **Multiannual Financial Framework** and related initiatives, including the **European Competitiveness Fund, defence procurement reform** and the emerging **Instrument for Strategic Enablers.**

1

Build a fast pathway from validated technology to operational deployment

Shorten the path from validation to deployment through coordinated test facilities, predictable accreditation and faster procurement.

2

Digital capabilities must be at the core of defence readiness

Treat AI, software, cyber resilience, drones and counter-drones, space, secure connectivity, cloud and trusted data as core defence capabilities and backbone infrastructure.

3

Make software-defined defence the guiding principle of Europe's capability development and procurement

Move from static platforms to secure, modular and interoperable systems that can integrate continuous upgrades.

4

Build a European defence market that aggregates demand, delivers scale and enables trusted cross-border deployment

Expand collaborative procurement, strengthen supply chains and reduce repeat testing through mutual recognition.

5

Make defence readiness a shared mission between governments, operational users and industry, backed by a resilient industrial base

Establish structured public-private cooperation, iterative capability development and industrial resilience.

1 Build a fast pathway from validated technology to operational deployment.

The European Union (EU) needs to radically shorten the time between successful validation and operational deployment. This requires the EU to bring existing national test facilities into a coordinated European network and give digital defence and dual-use companies, particularly SMEs and scale-ups, direct, free-of-charge access to testing and accreditation pathways. Testing should be based on predefined success criteria, with **results issued within four weeks of completing an agreed test scenario and accreditation decisions following predictable, time-bound procedures.**

Where a solution already meets recognised security certifications and assurance requirements, authorities should avoid duplicate assessment and focus on additional applicable defence-specific requirements. Successfully validated solutions, including those proven through paid pilots and exercises, should have a **credible and predictable pathway to follow-on and scaled procurement. Procurement processes should match the speed of technological development,** with proportionate tender and financial requirements, so that proven capabilities can move rapidly into operational use. **Progress should therefore be measured by the time from validation to operational deployment.**

2030 TARGET

By 2030, the **EU procurement and funding framework** should enable **fast-track pathways for validated digital defence and dual-use capabilities** at a **high Technology Readiness Level (TRL)** that meet applicable security requirements. Member States should be able to use these pathways individually or jointly, including through the European Defence Agency (EDA). **Procurement decisions should be taken within 4–6 months where feasible,** enabling successful solutions to move rapidly into follow-on procurement, including through joint arrangements where appropriate, and operational deployment.

2 Digital capabilities must be at the core of defence readiness.

Lessons from Ukraine show that modern military effectiveness and operational advantage on the battlefield increasingly depend on digital capabilities as strategic enablers. AI, software, cyber resilience, drones and counter-drones, space and autonomy should therefore be treated as core defence capabilities. Secure and interoperable connectivity, cloud and edge infrastructure, AI compute and trusted data infrastructure across appropriate classification levels should form the **trusted digital backbone** on which these capabilities depend. The backbone should include advanced 5G, progressively 6G, resilient diversified satellite connectivity, and space-based positioning, navigation and timing (PNT), linking strategic, operational and tactical environments. Where appropriate, the **EU and its Member States should systematically leverage dual-use technologies already proven at commercial scale** and secure them to defence requirements. **Cyber resilience should be treated as a continuous operational requirement,** rather than a point-in-time compliance exercise. These priorities should be reflected in European capability planning and investment.

2030 TARGET

By 2030, Europe should direct **25% of relevant new EU and national defence investment towards digital, emerging, disruptive and dual-use capabilities, including the trusted digital backbone and cyber resilience.**

3 Make software-defined defence the guiding principle of Europe's capability development and procurement.

Achieving defence readiness by 2030 cannot mean locking today's technology into platforms expected to operate for decades. The European Commission, working with Member States and EDA, should **promote software-defined defence as a guiding principle of capability development and procurement**. This means moving from static, platform-centric approaches to **secure, modular, and interoperable architectures** that allow continuous integration of software, AI, and other technologies throughout the capability lifecycle, including through upgrades to existing platforms. **This evolution also depends on secure and resilient digital infrastructure and connectivity.** Open standards and interoperable interfaces should be used where appropriate, while preserving controlled integration, system integrity and security. Underlying hardware architectures should also support technology insertion without requiring replacement of the entire platform, alongside continuous security monitoring and updates.

2030 TARGET

By 2030, **EU-supported collaborative defence capabilities** with significant digital content should apply **software-defined-by-design principles where appropriate.** These should be based on open and modular architectures with controlled integration, interoperable interfaces and continuous software and security-update pathways embedded in procurement and major upgrade cycles.

4 Build a European defence market that aggregates demand, delivers scale and enables trusted cross-border deployment.

The EU and its Member States cannot achieve readiness while defence demand and deployment remain fragmented along national lines. Member States should aggregate demand, align requirements, and expand collaborative procurement, **with a stronger role for EDA, giving industry the predictability to invest and scale.** This approach should be underpinned by **resilient supply chains and access to critical technologies and components**. Where this strengthens interoperability, security of supply and resilience, the EU should remain open to trusted and reliable international partners that operate and invest in Europe. **Cooperation should be based on transparent and verifiable security, supply-chain resilience and continuity requirements,** including the ability to operate, maintain and adapt capabilities throughout their lifecycle.

The EU should also enable secure cross-border deployment by establishing project-based mutual recognition. This should allow security controls, certifications and accreditation outcomes already validated in another participating Member State or trusted NATO environment to be recognised, where comparable levels of protection can be demonstrated. This should reduce unnecessary repeat testing and accreditation and strengthen EU–NATO interoperability, while preserving national security responsibilities. Over time, greater convergence of certification practices, supported by European and international standards, should reinforce this approach.



2030 TARGET

By 2030, at least **50% of defence procurement should be undertaken collaboratively,** supported by **project-basedmutual-recognition arrangements** that accelerate the deployment of validated digital capabilities across participating Member States **without unnecessary repeat testing or accreditation.**

5 Make defence readiness a shared mission between governments, operational users and industry, backed by a resilient industrial base

The EU needs to move from transactional industry consultation to mission-driven public-private cooperation. Governments and operational users should define strategic and operational needs, while **industry should be involved from the earliest stages of capability development to provide technological expertise, assess what can realistically be delivered and identify industrial constraints.** Capability development should be iterative, allowing technological options and operational experience to continuously inform testing, integration and upgrades.

To support this iterative approach, the European Commission and EDA should establish a **standing, secure mechanism for structured engagement with operational users and relevant industry.** This should bring together defence primes and system integrators, non-traditional defence companies, digital and dual-use technology providers, enabling-technology and component suppliers, SMEs, start-ups and scale-ups, as well as relevant industry associations where appropriate. The mechanism should provide input on technological developments, available capabilities, industrial capacity, critical dependencies and bottlenecks to delivery and scale. Where relevant, its insights should inform higher-level European security coordination. **Competent public authorities should retain strategic and operational decision-making.** The mechanism should also support the **continuity and resilience of the European Defence Technological and Industrial Base (EDTIB)** and its critical supply chains against cyber and hybrid threats. This should include **secure information-sharing between public authorities, operational users and industry, as well as coordinated stress-testing.** It should also **identify gaps in national protection approaches and support greater coordination.**



2030 TARGET

A standing, secure EU-level industry-engagement mechanism should be operational by 2028. By 2030, **EU-supported collaborative capability programmes** should systematically involve operational users and relevant industry from early capability development through testing and deployment to post-deployment feedback.



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 56,000 businesses who operate and invest in Europe. It includes 137 corporations which are global leaders in their field of activity, as well as 45 national trade associations from across Europe.

www.digitaleurope.org

@DIGITALEUROPE

@digitaleurope_org

DIGITALEUROPE