

14/02/2025

# Annex 1: Nine Policy Recommendations (challenges, solutions, examples)



## I. Europe's Defence Future Depends on Digitalisation – We Must Act Now

### 1. Protect critical entities and enable EU resilience through advanced technologies

**Challenges:** Modern conflicts demonstrate that a combination of inexpensive tools, such as drones, cyberattacks, and misinformation, can effectively disrupt critical infrastructures, paralysing economies and compromising military operational effectiveness. Critical entities, including health services, energy grids, transportation networks, and data centres, are particularly vulnerable to these hybrid threats. Unlike conventional warfare, digital attacks are continuous, requiring a proactive and integrated digital defence strategy, that bridges civilian and defence efforts, ensuring coordinated response mechanisms across both sectors.

**Solutions:**

- » **Strengthen EU Defence Resilience through a Competitive Digital Defence Programme:** Launch a competitive programme to drive innovation and development of advanced dual-use and critical technologies to safeguard critical entities from hybrid threats. This long-term initiative will prioritise creating secure connectivity and defence-ready solutions to protect critical entities. This programme should also **enhance coordination** between national security agencies, critical infrastructure operators, and defence bodies, ensuring a **unified response to hybrid threats**.
- » **Develop a Digital Defence Strategy to leverage advanced technologies to counter hybrid threats:** Employ cutting-edge technologies, including AI, next-generation communication systems, encrypted satellite links, robust cybersecurity tools, and drone defence systems, to detect, mitigate, and respond to hybrid threats targeting critical entities. This operational focus includes countering foreign information manipulation, interference (FIMI), and cognitive warfare campaigns. Given the private sector's continuous exposure to digital attacks and extensive expertise, structured collaboration with industry

is essential to enhance cyber resilience and ensure rapid threat response. Adopt a whole-of-society approach to enhance resilience through collaboration across government, private sector, civil society, and armed forces.

- » **Ensure the implementation of the NIS2 Directive and the Directive on the Resilience of Critical Entities:** These directives are vital for strengthening cybersecurity and resilience in critical sectors. However, delays in transposing these laws into national frameworks leave Europe vulnerable to cyberattacks and other risks. The EU must move from regulation to real-world security measures by ensuring effective enforcement and implementation. Positioning infrastructure protection as a dual-use priority will ensure that EU funds support cybersecurity investments that strengthen defence resilience.
- » **Harmonise security standards:** Align Member State security requirements with international standards to facilitate collaboration and interoperability across critical systems.

**Examples:** Recent drone strikes and cyberattacks on energy systems highlight the need for secure and resilient connectivity. Deploying encrypted networks and drone jamming systems can protect critical infrastructure and ensure operational continuity. AI-enhanced cybersecurity, including AI-supported pre-emptive countermeasures, leveraging telemetry across networks, cloud, and endpoints, can detect and neutralise cyberattacks on critical systems like power grids, preventing disruptions and strengthening resilience.

## 2. Advance digital defence and dual-use technologies

**Challenges:** The EU lags global leaders in adopting critical technologies like AI, quantum computing, cloud computing and 5G. Defence still operates with a "peacetime vs. wartime" mindset, whereas digital threats are continuous, requiring a shift to permanent cyber readiness.

### Solutions:

- » **Set digitalisation benchmarks:** Allocate 25 per cent of EU and NATO institutional funds and 25 per cent of Member States' new defence spending to advance digitalisation.
- » **Accelerate digital dual-use and critical digital technologies:** Earmark for investments in advanced technologies such as digital-twins, quantum computing, autonomous systems, next-generation communication technologies, e.g. 5G, satellite communication, cloud and edge computing, AI, big data, and additive manufacturing to drive civilian and military innovation and create the world's most flexible and modern defence capabilities. Enable real-time data based and software-defined defence solutions that are flexible and scalable.

- » **Modernise defence systems:** Replace legacy systems with modular, scalable and AI-driven cloud solutions to ensure rapid deployment and upgrades.
- » **Prioritise secure connectivity:** Strengthen trusted and pervasive connectivity through the EU toolbox (e.g. 5G) to ensure a resilient, future-ready infrastructure and robust digital backbone.

**Examples:** Investing in AI-powered maintenance, such as predictive maintenance, enhances operational readiness by minimising downtime. When advanced connectivity is available, it enables real-time data exchange, further improving efficiency. Machine learning, trained on IoT and IoMT data, predicts failures in sensors, vehicles, and weapons—allowing proactive maintenance and ensuring mission-critical systems remain operational.

Beyond maintenance, modular defence platforms, such as adaptable drones, extend operational flexibility. Equipped with interchangeable payloads, these systems can switch roles, reducing costs and maximising use. Similarly, secure satellite communication powered by small GEO and Earth observation satellites enhances real-time intelligence, providing AI-driven object detection, change monitoring, and map updates for EU defence and security.

In this context, the EU can develop a European Drone Ecosystem to strengthen supply chain security, drive innovation, and enhance interoperability. Collaborative research programs can bring together SMEs and major manufacturers to create open-architecture drone platforms that seamlessly integrate into EU defence and civilian infrastructure.

### 3. Address the digital defence skills gap

**Challenges:** The EU faces a critical shortage of skilled professionals in areas like AI and cybersecurity. Barriers to talent mobility, inconsistent security clearance standards and uncompetitive career opportunities exacerbate workforce challenges, weakening the defence sector's capacity.

#### **Solutions:**

- » **Expand digital skills initiatives:** Implement EU-funded training programmes focused on AI, cybersecurity and connectivity, targeting all levels of military organisations whilst pooling and promoting existing initiatives by Member States and companies.
- » **Foster talent mobility:** Introduce a European Digital Skills Passport to streamline qualification recognition and facilitate cross-border workforce mobility. Address barriers such as inconsistent security clearance standards and restrictive national laws. Expanding participation in cross-border cyber defence exercises will enhance skills development and public-private cooperation.

- » **Partner for training platforms:** Collaborate with industry, academia and research organisations to co-develop training aligned with evolving digital defence needs.
- » **Retain skilled professionals:** Develop EU-wide policies to enhance career opportunities, offering competitive salaries and clear growth pathways to retain talent in the defence sector.

**Examples:** A European Digital Skills Passport can enable faster upskilling and hiring across borders. For instance, a cybersecurity contractor could quickly deploy certified personnel from another EU country during a crisis.



## II. A single European defence market is key for speed and scale

### 4. Establish a Single defence market for technological competitiveness

**Challenges:** The EU defence market is fragmented due to diverse national regulations, procurement processes and workforce policies, limiting cross-border collaboration and increasing costs. SMEs and mid-sized enterprises face significant barriers, struggling with complex procurement systems and fragmented standards. The lack of interoperability across defence systems, harmonised investment and workforce mobility undermines the EU's ability to act collectively in crisis scenarios, increasing duplication and inefficiencies.

#### **Solutions:**

- » **Harmonise regulations and reduce fragmentation:** Develop a single EU defence market by aligning accreditation and procurement standards whilst respecting national defence policies. This will enable cross-border collaboration and innovation in digital technologies.
- » **Develop a Common Defence Digital Backbone to Strengthen Interoperability:** Establish interoperability as a core KPI for defence digitalisation across the EU and Allies, ensuring seamless coordination across land, sea, air, space, and cyber domains. Develop a standardised digital infrastructure to enable secure communication, cloud-based data sharing, AI-driven decision-making, and effective joint operations.
- » **Streamline investment processes:** Attract private financing and encourage long-term growth in critical technologies. Create mechanisms to improve workforce mobility across Member States by removing barriers to hiring and transferring skilled personnel.
- » **Simplify and digitalise procurement:** Introduce dynamic digital marketplaces to reduce administrative burdens and promote SME participation. Support joint design and procurement initiatives to enhance R&D and production efficiency. Further simplifying

procurement and research access for SMEs will foster innovation across the defence sector.

**Examples:** Harmonising defence procurement regulations would allow a manufacturer of defence or dual-use technologies—such as secure communication devices, sensors, and autonomous systems—to supply standardised products across Member States, reducing costs and deployment timelines.

## 5. Promote joint procurement to strengthen the defence market and drive innovation

**Challenges:** Fragmented national procurement systems prevent economies of scale, increase costs and delay the adoption of commercially available technologies. Defence procurement cycles lag significantly behind commercial technology innovation, limiting Europe's ability to integrate cutting-edge digital solutions at scale.

### Solutions:

- » **Scale joint procurement across the EU:** Streamlined EU-wide procurement initiatives to consolidate demand, reduce costs and ensure adoption of interoperable technologies would foster a competitive European defence market at scale.
- » **Accelerate technology adoption through agile procurement:** Use joint procurement to fast-track the adoption of critical digital technologies like cloud infrastructure and AI systems. Align defence procurement timelines with commercial innovation cycles to enhance operational agility.

**Example:** Joint procurement can significantly lower the per-unit cost of dual-use technologies. For instance, bulk orders for secure cloud-based infrastructure enable Member States to share data securely whilst enhancing operational effectiveness.

## 6. Accelerate production capabilities and resilient supply chains through earmarking investment

**Challenges:** Outdated manufacturing systems and overreliance on non-EU suppliers expose vulnerabilities in critical supply chains. Defence production struggles to match the speed of commercial innovation, delaying the adoption of advanced technologies. Whilst trusted vendors and partners outside the EU will remain essential to supply chain resilience, strengthening Union's domestic production capabilities and fostering diverse, secure partnerships across allied nations is a strategic necessity.

### Solutions:

- » **Fast-track defence production and standardise supply chains:** Accelerate the adoption of advanced defence technologies by

streamlining procurement and scaling up production. Establish common digital manufacturing and supply chain standards to ensure interoperability across Member States and Allies, reducing duplication and improving efficiency.

- » **Invest in modernising and digitalising EU defence production capabilities** by adopting advanced technologies such as secure connectivity, advanced energy supply, drone jamming, AI, robotics, 3D printing and digital twins. These technologies will improve scalability, quality and efficiency whilst fostering a digitally skilled workforce.
- » **Diversify supply chains** by fostering partnerships within and beyond the EU, ensuring access to critical technologies and strengthening collaboration with allied defence and industry stakeholders.
- » **Develop robust, cyber-resilient production systems** to withstand disruptions. Incorporate backup mechanisms to ensure continuity during crises.

**Examples:** By adopting AI-driven robotics and additive manufacturing, supported by secure and high-speed connectivity where needed, EU defence industries can increase reliability and efficiency while maintaining scalability and quality during supply chain disruptions. Technologies like Extended Reality (XR) can accelerate prototyping, allowing engineers to test designs in immersive environments.



### III. Stronger defence partnerships with NATO, US and Ukraine

#### 7. Enhance collaboration with Ukraine on technologies and innovation

**Challenges:** The war in Ukraine has disrupted its defence industry, underscoring the need to integrate Ukraine's defence technological and industrial base into the European defence ecosystem. This integration offers an opportunity to foster resilience, interoperability and innovation.

**Solutions:**

- » **Establish an EU-Ukraine partnership** under the permanent structured cooperation in defence (PESCO) and the European Defence Fund (EDF) to enable joint projects between ministries of defence, industry and research institutions, focusing on innovative and interoperable technologies like AI-driven analytics and autonomous systems.
- » **Develop digital and technological hubs in Ukraine:** Create centres of excellence in strategic locations to support R&D, training and prototyping. These hubs would also act as repair and logistics facilities for advanced defence technologies and foster EU-Ukraine industrial integration.

- » **Expand funding and investments:** Leverage EDF and EIB instruments to support joint R&D projects, ensuring scalability and dual-use potential whilst facilitating Ukraine's industrial modernisation and economic recovery.

## 8. Strengthen EU-NATO collaboration on Digital Security and Defence Interoperability

**Challenge:** Inconsistent standards and communication protocols limit seamless EU-NATO collaboration. Inadequate interoperability of systems and dual-use technologies reduce the effectiveness of joint missions and collective efforts against hybrid threats.

### Solutions:

- » **Strengthen Civilian-Military-Industry Coordination for Hybrid Threats:** Establish a structured framework to bridge the gap between civilian and military defence, ensuring clearer roles and joint operational models for responding to hybrid threats, including cyber, information warfare, and critical infrastructure disruptions. Enhance structured dialogue with industry and critical infrastructure operators to integrate real-world threat intelligence, ensuring EU-NATO strategies remain adaptive and informed by evolving risks.
- » **Harmonise standards for interoperability:** Collaborate with NATO to standardise dual-use technologies, ensuring seamless interoperability across defence-related technology assets and leveraging best practices in cyber resilience and operational coordination.
- » **Foster joint initiatives:** Collaborate on projects addressing hybrid threats, secure communications, digital resilience and advanced R&D to strengthen collective defence capabilities. Joint cyber exercises can strengthen interoperability, improve crisis preparedness, and enhance cooperation between public and private actors.
- » **Enhance mission integration with AI:** Develop harmonised tools for real-time communication (e.g. 5G) and AI-powered decision-making to enhance joint missions. Applications such as predictive logistics and battlefield analytics will optimise outcomes and improve operational interoperability.

**Examples:** Aligning EU-NATO standards for communication protocols, such as '5G for Defence', would enhance interoperability and ensure seamless data sharing during collaborative military missions. This would strengthen information superiority and improve response effectiveness against hybrid threats.

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

**Challenge:** Dual-use and critical technologies are rapidly reshaping defence and security. However, fragmented regulations, varying standards, and limited transatlantic coordination pose challenges to unlocking their full potential. Without stronger collaboration, the EU and US risk inefficiencies in addressing shared threats such as cyberattacks and supply chain vulnerabilities.


**Solutions:**

- » **Establish the EU-US Dual-Use and Critical Tech Council (DCTC):** Create a permanent transatlantic platform to strengthen collaboration on dual-use technologies. The DCTC would harmonise policies, foster dialogue on critical technologies, and align regulations to enhance interoperability and innovation.
- » **Launch Joint Investment Programmes for Dual-Use Technologies:** Transatlantic funding initiatives should be established to drive collaborative innovation in critical areas such as AI, cybersecurity, drones, and quantum technologies. These technologies are essential to ensuring joint battlefield superiority and operational effectiveness.

**Examples:** The DCTC could facilitate the development of secure quantum communication systems that support both civilian and military networks, ensuring resilience against cyberattacks while enabling seamless transatlantic coordination during crises.



FOR MORE INFORMATION, PLEASE CONTACT:

 **Constantinos Hadjisavvas**

**Director for Digital Resilience and Defence**

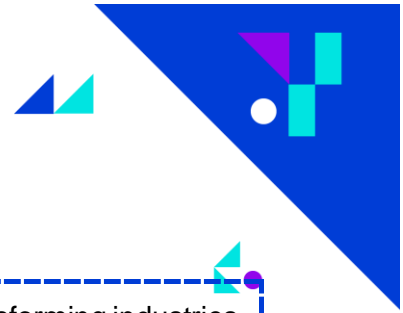
[constantinos.hadjisavvas@digitaleurope.org](mailto:constantinos.hadjisavvas@digitaleurope.org) / +32 488 57 10 61

---

 **Milda Basiulyte**

**Senior Director for Cyber, Infrastructure, Competitiveness & Digital Transformation**

[milda.basiulyte@digitaleurope.org](mailto:milda.basiulyte@digitaleurope.org) / +32 493 89 20 59



## About 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 113 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.