Prepared by DigitalTrade4.EU

Strengthening Europe's Resilience and Competitiveness through Digital Interoperability and Security

June 2025

About Us

The **DigitalTrade4.EU consortium** envisions a **seamlessly interconnected Europe** and **neighbouring regions** powered by harmonized standards for the digitalisation of trade documents and processes. By fostering the digital transformation of trade, we aim to promote economic integration, enhance cooperation, and ensure long-term trade facilitation across borders.

Our consortium is made up of **experts in their field**, including **105 full partners**—trade associations, logistics providers, shipping lines, banks and insurances, technology innovators, etc.—**from 17 European Union countries** (*France, Belgium, Netherlands, Austria, Estonia, Finland, Italy, Latvia, Spain, Germany, Sweden, Poland, Luxembourg, Lithuania, Slovenia, Denmark, Bulgaria*) and **22 non-EU countries** (*United Kingdom, Switzerland, Montenegro, Japan, Singapore, Hong Kong, Australia, New Zealand, India, Nepal, Canada, United States of America, Cameroon, Morocco, Egypt, Kenya, Pakistan, Nigeria, Brazil, Uzbekistan, Turkey, Ukraine*).

Our consortium is already **aligned with the fundamentals** of the **EU Competitiveness Compass**. Learn more:

- How DigitalTrade4.EU Can Help Achieve the Objectives of the EU Competitiveness Compass (February 2025) https://www.digitaltrade4.eu/how-digitaltrade4-eu-can-help-achieve-the-objectives-of-the-eu-competitiveness-compass/

Web page: www.digitaltrade4.eu

EU Transparency Register: 355266197389-94

Contact person: Riho Vedler

Email: riho.vedler@ramena.ee

Executive Summary

DigitalTrade4.EU welcomes the **European Commission**'s proactive stance on strengthening the Union's **cybersecurity posture** through the revision of the **Cybersecurity Act (CSA)** and bolstering its **defence capabilities** as outlined in the **"*JOINT WHITE PAPER for European Defence Readiness 2030*[1]".** In an era of increasing **geopolitical volatility** and **sophisticated digital threats**, a cohesive and **forward-looking strategy** is paramount.

This **feedback** underscores the **critical role** of **interoperability** and **decentralisation** as **foundational principles** to achieve the **EU's objectives** in **digital trade, cybersecurity,** and **defence**. These principles enable **'dual-use' solutions—technologies** and **frameworks** that serve both **civilian** and **military purposes**, such as **secure logistics platforms** for **trade** and **troop movements**. For instance, **decentralized logistics platforms** could simultaneously **streamline** commercial **supply chains** and coordinate **NATO troop deployments**, while **Digital Product Passports (DPPs)** might **track** both **commercial goods** and **critical defence components**.

By fostering **harmonized digital standards** and **resilient, decentralised systems**, the EU can significantly enhance its **strategic autonomy, economic competitiveness,** and the **security** of its **citizens and infrastructure**.

DigitalTrade4.EU believes that integrating these principles, drawing on values of **solidarity, collective action,** and **technological innovation** highlighted in the **Defence White Paper**, will create a more **secure, efficient,** and **resilient European digital ecosystem**.

Our **recommendations** aim to align the **Commission's goals** with **practical, future-proof solutions** that leverage the **transformative potential** of **digital technologies** for both **civilian and defence applications**.

Note: *In this document, the terms* ***Small and Medium-sized Enterprises (SMEs)*** *and* ***Micro, Small and Medium-sized Enterprises (MSMEs)*** *are used interchangeably and carry the same meaning and weight. This clarification is important because different sources and contexts may refer to these groups using either acronym, but both encompass the full range of smaller business categories critical for economic development.*

[1] European Commission. Joint White Paper for European Defence Readiness 2030 (March 2025) https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf

Introduction

DigitalTrade4.EU is a **consortium** dedicated to fostering a **seamlessly interconnected Europe** and **neighbouring regions**, powered by **harmonized standards** for the **digitalisation** of **trade documents** and **processes**. Our **mission** is to **promote economic integration, enhance cooperation,** and **ensure long-term trade facilitation** across borders, contributing to the **EU's green and digital twin transitions**.

The current **geopolitical landscape**, coupled with the **rapid evolution** of **digital technologies** and **threats**, necessitates a **robust** and **integrated European response**. The **Commission's initiative** to **revise the Cybersecurity Act** and the **strategic vision** presented in the **"*JOINT WHITE PAPER for European Defence Readiness 2030*"** are **timely** and **crucial**. The **White Paper**'s call to **"re-arm Europe"** and build a **"strong and innovative defence industry"** resonates with the need for **underlying digital frameworks** that are **secure, resilient,** and **interoperable**.

This **document** provides **DigitalTrade4.EU**'s perspective on how the principles of **interoperability** and **decentralisation** can be **strategically embedded** within the **EU's evolving cybersecurity** and **defence frameworks**.

We believe that our **expertise** in **digital trade & logistics standards** and **infrastructure** can offer **valuable insights** into creating **synergies** between **economic prosperity, robust security,** and **enhanced defence readiness**, aligning with the **Commission's simplification agenda** and the **imperative for a more resilient Union**.

Expectations from the Commission's Side: The Objectives

DigitalTrade4.EU acknowledges the comprehensive objectives set forth by the European Commission across the cybersecurity and defence domains. **Regarding the Revision of the Cybersecurity Act (CSA), the Commission aims to:**

- **Streamline cybersecurity measures and strengthen cyber resilience:** Adapting ENISA's mandate to its evolved position and tasks in a complex cybersecurity landscape, ensuring it can proactively address emerging threats like ransomware and supply chain attacks.
- **Improve the European Cybersecurity Certification Framework (ECCF):** Enhancing the adoption process, agility, effectiveness, and clarity of roles, including the maintenance of certification schemes and addressing non-technical risk factors.
- **Address ICT supply chain security challenges:** Strengthening the security of ICT supply chains against internal and external threats.
- **Promote simplification:** Reducing administrative burden and ensuring a business-friendly environment by simplifying cybersecurity-relevant requirements across legislation.

Regarding the European Defence Readiness 2030, the Commission and High Representative call for:

- **Re-arming Europe:** A massive, coordinated increase in European defence spending and capabilities to deter aggression and secure Europe's future.
- **A stronger and more resilient defence industrial base:** Fostering an ecosystem of technological innovation and ensuring the security of supply.
- **Addressing critical capability gaps:** Through collaborative projects and EU incentives, particularly in areas like air and missile defence, artillery, ammunition, drones, military mobility, AI, Quantum, Cyber & Electronic Warfare, and strategic enablers.

- **Enhanced military support for Ukraine:** Strengthening Ukraine's defence capacity as a frontline of European defence.
- **Regulatory simplification and harmonisation:** Through initiatives like the "Defence Omnibus Simplification proposal" to improve the agility of the European Defence Technological and Industrial Base (EDTIB).
- **Fostering collaboration and interoperability:** To generate economies of scale, improve delivery timelines, and enhance the effectiveness of Member States' efforts, including contributions to NATO.

Common threads across these objectives include the pursuit of enhanced **resilience, security, strategic autonomy, technological leadership, simplification, and the critical need for coordinated, EU-wide action** that leverages both public and private sector capabilities.

Approach and Recommendations

DigitalTrade4.EU advocates for an approach rooted in the principles of **interoperability and decentralisation** to effectively meet the Commission's objectives in cybersecurity and defence, while simultaneously bolstering the EU's digital single market and trade competitiveness. **Our vision for green-digital trade, built on harmonized legal frameworks and standards like the UNCITRAL Model Law on Electronic Trade-Related Documents (MLETR)[2], the UNECE Recommendation No. 49 ("Transparency at Scale")[3], the revised eIDAS Regulation (eIDAS 2.0)[4], and Digital Product Passports (DPPs)[5], which enable secure cross-border transactions, trusted digital identities, and product traceability**.

Leveraging Interoperability and Decentralisation for Defence Readiness

The "***JOINT WHITE PAPER for European Defence Readiness 2030***" emphasizes values such as **solidarity, collective action, resilience, credible deterrence, technological innovation, efficiency, interchangeability, and security of supply**. Interoperability and decentralisation are key enablers for these values:

- **Enhanced Military Mobility and Logistics:** Interoperable digital systems for trade and logistics (e.g., based on eFTI, MLETR) can be dual-use, facilitating the seamless and secure movement of troops, equipment, and supplies across borders, as prioritized in the White Paper. Decentralised data exchange platforms can enhance the resilience of these logistics chains against targeted attacks.
- **Resilient Defence Supply Chains:** The digitalisation of trade documents and the implementation of DPPs can enhance the traceability, security, and resilience of

[2] UNCITRAL. Model Law on Electronic Transferable Records
https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
[3] United Nations Economic and Social Council. Recommendation No. 49: Transparency at Scale – Fostering Sustainable Value Chains (March 2025)
https://unece.org/sites/default/files/2025-05/ECE-TRADE-C-CEFACT-2025-03E.pdf
[4] European Commission. Discover eIDAS
https://digital-strategy.ec.europa.eu/en/policies/discover-eidas
[5] European Commission. EU's Digital Product Passport: Advancing transparency and sustainability
https://data.europa.eu/en/news-events/news/eus-digital-product-passport-advancing-transparency-and-sustainability

defence supply chains. Knowing the provenance and journey of critical components is vital. Decentralised ledger technologies can provide immutable records, increasing trust and security.

- **Collaborative Defence Projects and "Collaborative Dividend":** True collaboration in developing and procuring defence capabilities, as called for in the White Paper, hinges on the ability to securely and efficiently share information and data. Interoperable communication and data exchange standards are fundamental. Decentralised systems can allow for secure collaboration environments without single points of failure.
- **Strengthening the EDTIB:** A "strong and innovative defence industry" requires a robust digital backbone. Secure cross-border data flows, trusted digital identities (eIDAS 2.0), and high cybersecurity standards – principles DigitalTrade4.EU champions for digital trade – are equally critical for the EDTIB. This supports the White Paper's aim to "facilitate the exchange of confidential and sensitive information under conditions that ensure both simplicity and security of handling."
- **Supporting Strategic Capabilities (AI, Quantum, Cyber):** The development and deployment of advanced capabilities like AI, Quantum computing, and cyber defence tools require secure and interoperable data frameworks. Decentralised data architectures can offer enhanced security and control for sensitive data used in these domains.

Aligning with the Cybersecurity Act Revision

DigitalTrade4.EU's focus on robust digital standards and infrastructure directly supports the objectives of the CSA revision:

- **Effective European Cybersecurity Certification Framework (ECCF):** Interoperable standards for digital products and services, as advocated by DigitalTrade4.EU, can simplify the development and mutual recognition of cybersecurity certifications. Our work on promoting secure and standardized digital trade practices aligns with the need to enhance the security of ICT supply chains.
- **Resilience through Decentralisation:** Decentralised digital infrastructures are inherently more resilient to certain types of cyberattacks (e.g., DDoS, single-point-of-

failure exploits) than centralised ones. Promoting decentralised models for critical information systems can contribute significantly to the EU's overall cyber resilience.

- **Simplification and Harmonisation:** The adoption of common, interoperable digital standards (MLETR, eIDAS 2.0, DPPs) across the EU simplifies compliance for businesses and authorities alike. This aligns with the Commission's simplification agenda and the "Defence Omnibus Simplification proposal" by reducing regulatory fragmentation.

Specific Recommendations

1. Champion EU-wide Adoption of Interoperable Digital Standards for Dual Use

- Actively promote and mandate where appropriate the use of **UNCITRAL MLETR, eIDAS 2.0 (Electronic Identification, Authentication, and Trust Services), and the eFTI[6] (Electronic Freight Transport Information) regulation** not only for commercial trade but also as foundational layers for secure data exchange in defence logistics, critical infrastructure management, and public administration.
- Ensure that the **European Digital Identity Wallet** is designed with the necessary security features and interoperability to support secure access and authentication in sensitive sectors, including defence.

2. Extend Digital Product Passports (DPPs) for Defence and Critical Components

- Adapt and extend the **DPP framework** to cover critical components within the defence supply chain and other critical infrastructures. This would enhance traceability, verify authenticity, track maintenance, and ensure compliance with security and ethical sourcing standards.
- Link DPP data with secure, interoperable platforms to provide real-time visibility and risk assessment capabilities.

[6] European Commission Transport and Mobility. Electronic freight transport information (eFTI) https://transport.ec.europa.eu/transport-themes/logistics-and-multimodal-transport/efti-regulation_en

3. **Promote Decentralised Architectures for Critical Systems**

   - Encourage and fund research and deployment of **decentralised digital infrastructures** (e.g., based on DLT, peer-to-peer networks) for critical data exchange, communication systems, and command and control networks to enhance resilience against cyberattacks and ensure operational continuity.
   - Explore decentralised models for the **ECCF** to improve its agility and resilience.

4. **Invest in Dual-Use Digital Infrastructure**

   - Prioritize investments under programs like the Connecting Europe Facility (CEF) and Digital Europe Programme in digital infrastructure projects that serve **both civilian and defence needs**. This includes secure communication networks, data centres, and cloud infrastructure built on principles of interoperability and security-by-design.
   - Extend the concept of **military mobility corridors** to include robust and resilient digital corridors, ensuring secure data flow alongside physical movement.

5. **Foster Public-Private Partnerships for Secure and Interoperable Solutions**

   - Establish frameworks and funding mechanisms to encourage **collaboration between public authorities (including defence agencies) and the private sector** (including DigitalTrade4.EU members) in developing and deploying secure, interoperable digital solutions for trade, cybersecurity, and defence.
   - Launch **pilot projects** that demonstrate the benefits of integrating digital trade solutions (e.g., paperless logistics, secure e-identities) with defence supply chain management and cybersecurity protocols.

6. **Integrate Cybersecurity into Digital Trade Agreements and Standards**

   - Ensure that EU digital trade agreements and international standardisation efforts consistently promote high levels of cybersecurity, data protection, and resilience, drawing from the revised CSA and ENISA's expertise. This reinforces the EU's role as a global standard-setter.

7. Support Simplification through Digitalisation

- Recognize that the widespread adoption of harmonized digital processes and standards is a powerful tool for simplification, reducing administrative burdens for businesses (including SMEs in the defence sector) and public administrations. For example, digital customs procedures compliant with MLETR can cut compliance costs for SMEs by 30–40% compared to paper-based systems. Ensure the "Defence Omnibus Simplification proposal" fully leverages digital transformation.

Conclusion and Next Steps

DigitalTrade4.EU is firmly committed to supporting the European Commission in achieving a more secure, resilient, and competitive Union. We believe that the strategic implementation of **interoperability and decentralisation** across digital trade, cybersecurity, and defence is not merely an option but a necessity for navigating the complexities of the modern world. These principles offer a pathway to enhanced strategic autonomy, operational efficiency, and robust security, aligning perfectly with the core values and objectives articulated by the Commission.

By embracing harmonized digital standards and fostering resilient, decentralised systems, the EU can unlock significant synergies, ensuring that advancements in one domain positively reinforce others. This integrated approach will be crucial for the success of the revised Cybersecurity Act, the ambitions of the European Defence Readiness 2030 strategy, and the overall prosperity and security of the European Union.

DigitalTrade4.EU proposes the following next steps for collaboration:

- **Engage in a structured dialogue** with DG CNECT, DG DEFIS, EEAS, and ENISA to further elaborate on the practical implementation of these recommendations.
- **Participate in relevant expert groups and consultations** concerning the CSA revision, ECCF development, and defence industrial strategy, bringing our expertise on digital standards and interoperability.
- **Collaborate on pilot projects** that test and showcase the application of interoperable and decentralised digital solutions in dual-use contexts, particularly in secure logistics and supply chain management.
- **Contribute to awareness-raising and capacity-building initiatives** to promote the adoption of secure and interoperable digital practices among businesses and public authorities across the EU.
- **SMEs** constitute over **99%** of **EU businesses** and are **critical** to **supply chain resilience**. Their participation in **decentralised digital systems** (e.g., DLT-based platforms based on Zero Trust Architecture) **reduces fragmentation** and **strengthens collective cybersecurity**.

We are confident that by working together, we can build a digital future for Europe that is both innovative and secure, prosperous and resilient.