Prepared by DigitalTrade4.EU

Feedback to the European Commission on Defence Readiness and Industrial Strategy

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** and **strongly supports** the European Commission's **ambitious initiatives** to bolster the European Union's **defence capabilities**, as outlined in the "**JOINT WHITE PAPER for European Defence Readiness 2030**[1]" and the **COM(2025) 188 final**[2] (*Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2021/694, (EU) 2021/695, (EU) 2021/697, (EU) 2021/1153, (EU) 2023/1525 and 2024/795, as regards incentivising defence-related investments in the EU budget to implement the ReArm Europe Plan*).

We believe that a **resilient, technologically advanced, and interoperable defence sector** is crucial for the EU's **strategic autonomy and security** in the current geopolitical landscape. This feedback highlights the **critical role** that **digital transformation**—particularly through the principles of **interoperability, decentralisation, and harmonised international standards**—can play in achieving the EU's **defence objectives**.

DigitalTrade4.EU asserts that many of the **secure**, **efficient**, and **resilient** digital trade solutions we promote—such as **electronic transferable records** compliant with **UNCITRAL Model Law on Electronic Transferable Records (MLETR)**[3], **interoperable digital identities** under **EU eIDAS 2.0 Regulation**[4], and **UNECE Recommendation No. 49 ("Transparency at Scale")**[5] for **Digital Product Passports (DPPs)**—possess significant **dual-use potential**, meaning they can serve both **civilian economic purposes** and **military defence applications**.

For instance, **MLETR-compliant electronic bills of lading** used in commercial shipping can be adapted to secure **cross-border military logistics documentation**, while **eIDAS 2.0 digital**

[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

[2] European Commission. Mini omnibus for defence, Commission adoption https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14697-Mini-omnibus-for-defence_en

[3] UNCITRAL. Model Law on Electronic Transferable Records https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

[4] European Commission. Discover eIDAS https://digital-strategy.ec.europa.eu/en/policies/discover-eidas

[5] 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

identities can authenticate defence contractors accessing sensitive installations. **DPPs tracking carbon footprints in civilian supply chains** can similarly trace ballistic missile components to prevent counterfeiting. These solutions have the capability to enhance both the **EU's economic competitiveness** and its **defence readiness**.

By **strategically leveraging digital technologies** for logistics, supply chain management, secure data exchange, and critical component traceability, the EU can significantly enhance its **European Defence Technological and Industrial Base (EDTIB)**, improve **military mobility**, and ensure the **security of supply** for its defence needs. Our recommendations focus on **integrating these digital principles** into the EU's defence strategy to create a **more secure, efficient, and technologically sovereign European defence ecosystem**.

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 **rapidly evolving geopolitical environment** and the **increasing sophistication of threats** underscore the timeliness and importance of the Commission's White Paper on European Defence Readiness 2030 and the accompanying regulatory proposals. The call to "**re-arm Europe**," strengthen the **EDTIB**, and address **critical capability gaps** requires a multifaceted approach where **digital transformation is a key enabler**.

This document provides DigitalTrade4.EU's perspective on how the **strategic adoption of interoperable and decentralised digital frameworks**, already proving beneficial in trade and logistics, can significantly contribute to the EU's **defence and security ambitions**. We aim to **align our expertise** in digital standards, secure data exchange, and supply chain digitalisation with the Commission's objectives, offering **actionable recommendations** that support a **stronger, more resilient, and technologically advanced European defence posture**.

Expectations from the Commission's Side: The Objectives

DigitalTrade4.EU has **carefully reviewed** the Commission's strategic documents and acknowledges the **comprehensive and urgent objectives** set forth.

From the COM(2025) 188 final, we note key objectives including:

- **Incentivising significant defence-related investments** via the EU budget to implement the **ReArm Europe Plan**.
- Extending the **Strategic Technologies for Europe Platform (STEP)**[6] to encompass **defence-related technologies and products**.
- Amending key EU funding programmes (**European Defence Fund - EDF, Digital Europe Programme - DEP, Horizon Europe - HE, Act in Support of Ammunition Production - ASAP, Connecting Europe Facility - CEF**) to better support **defence investments, dual-use projects, and the EDTIB**.
- Strengthening the **competitiveness, innovation, and technological autonomy** of the **European Defence Technological and Industrial Base (EDTIB)**.
- Enhancing **military mobility** and the development of **dual-use transport infrastructure**.
- Facilitating **cumulative funding and transfers of resources** to defence-related initiatives.

From the "JOINT WHITE PAPER for European Defence Readiness 2030" (JOIN(2025) 120 final), we identify overarching goals such as:

- **Re-arming Europe:** Achieving **sufficient military readiness and capabilities by 2030** to **credibly deter aggression** and secure Europe's future.

[6] European Union. Strategic Technologies for Europe Platform https://strategic-technologies.europa.eu/index_en

- **Strengthening the Defence Industrial Base:** Fostering a **strong, resilient, and innovative EDTIB** with **secure supply chains**.
- **Addressing Critical Capability Gaps:** Collaboratively tackling shortfalls in areas such as **air and missile defence, artillery systems, ammunition and missiles, drones and counter-drone systems, military mobility, AI, Quantum, Cyber & Electronic Warfare, and strategic enablers**.
- **Enhanced Military Support for Ukraine:** Stepping up assistance and integrating Ukraine's defence industry where appropriate.
- **Regulatory Simplification and Harmonisation:** Implementing measures like the "**Defence Omnibus Simplification proposal**" to increase the **agility of the EDTIB** and **streamline procurement**.
- **Fostering Collaboration and Interoperability:** Generating **economies of scale**, improving **delivery timelines**, and enhancing the **effectiveness of Member States' efforts**, including contributions to NATO.
- **Increasing Defence Spending:** A **massive, coordinated surge** in European defence investment over a **sustained period**.
- **Reducing Dependencies and Ensuring Security of Supply:** Identifying **critical raw materials and components** and **diversifying supply sources**.

DigitalTrade4.EU understands these objectives as a **clear call** for a **more integrated, technologically advanced, and strategically autonomous European defence framework**. Our approach and recommendations are geared towards supporting these ambitions through the **transformative power of digitalisation**.

Approach and Recommendations

DigitalTrade4.EU advocates an approach based on **interoperability**, **decentralisation**, and the adoption of **harmonised international digital standards**—principles vital to strengthening the EU's **digital single market** and trade competitiveness, while offering significant **dual-use potential** to support the Commission's defence and security goals.

Our vision for **green-digital trade** leverages frameworks such as the **MLETR**, the revised **EU eIDAS 2.0 Regulation**, the **EU Electronic Freight Transport Information Regulation (eFTI)**[7], and **Digital Product Passports (DPPs)** to enable **secure**, **traceable**, and **efficient** cross-border data and goods flows.

MLETR provides a legal basis for transferable trade documents—like **bills of lading**, **promissory notes**, and **warehouse receipts**—to be issued and transferred electronically with the same legal effect as paper documents, thereby modernizing trade, reducing **fraud risk**, and accelerating commerce. Complementing this, eIDAS 2.0 establishes a harmonised EU framework for **electronic identification** and **trust services**. Together, these standards form the backbone of a **secure**, **interoperable**, and **legally recognized** digital ecosystem—essential not only for commercial trade but also for the increasingly complex defence supply chains.

Leveraging Interoperability and Decentralisation for Defence Readiness

The values highlighted in the Defence White Paper—**solidarity, collective action, resilience, credible deterrence, technological innovation, efficiency, interchangeability, and security of supply**—can be **significantly enabled by digital transformation**.

1. **Enhanced Military Mobility and Logistics**

    - **Recommendation:** Promote and adapt **interoperable digital systems** developed for trade and logistics (e.g., based on eFTI, MLETR) for **dual-use in defence**. This can facilitate the **seamless, secure, and rapid movement of**

[7] European Commission, Mobility and Transport. eFTI Regulation, Digitalising freight transport across the European Union
https://transport.ec.europa.eu/transport-themes/logistics-and-multimodal-transport/efti-regulation_en

troops, equipment, and supplies across borders, directly addressing a key priority of the White Paper and the CEF amendments.

- **Benefit:** **Decentralised data exchange platforms** can enhance the **resilience of military logistics chains** against targeted attacks or disruptions. By **distributing data control** across **multiple nodes**, **decentralised platforms** reduce the risk of **single points of failure** and make **cyberattacks** more difficult to **execute successfully**, thereby enhancing **operational continuity**.

2. **Resilient and Secure Defence Supply Chains**

   - **Recommendation:** Extend the concept of **Digital Product Passports (DPPs) to critical defence components and materials**. This enhances **traceability, verifies authenticity, tracks maintenance lifecycles, and ensures compliance** with security and ethical sourcing standards for the EDTIB.

   - **Benefit:** **Distributed Ledger Technology (DLT)**, such as **blockchain**, enables **secure, tamper-proof** record-keeping across **distributed networks**. Unlike **centralised systems**, **DLT eliminates single points of failure**, making **supply chain data** resilient to **cyberattacks** and **unauthorized alterations**, thereby ensuring **data integrity** and **trustworthiness**. This aligns with the White Paper's emphasis on securing supply chains against disruptions.

3. **Collaborative Defence Projects and the "Collaborative Dividend"**

   - **Recommendation:** Foster the development and adoption of **secure and interoperable communication and data exchange standards** for collaborative defence projects. This is **fundamental** to achieving the "**collaborative dividend**" envisioned in the White Paper.

   - **Benefit:** **Decentralised systems** can create **secure collaboration environments** for research, development, and procurement among Member States and trusted partners, **without creating single points of failure**.

4. **Strengthening the European Defence Technological and Industrial Base (EDTIB)**

   - **Recommendation:** Support the EDTIB with a **robust digital backbone** built on **secure cross-border data flows, trusted digital identities (leveraging eIDAS 2.0), and high cybersecurity standards**. This aligns with the White Paper's aim to **"facilitate the exchange of confidential and sensitive information under conditions that ensure both simplicity and security of handling."**
   - **Benefit:** **SMEs within the defence supply chain** can particularly benefit from **simplified and secure digital interaction and procurement processes**.

5. **Enhancing Secure Identity and Access Management for Defence**

   - **Recommendation:** Leveraging the **European Digital Identity Wallet** developed under **eIDAS 2.0** to provide **trusted**, **interoperable digital identities** for **defence personnel** and **contractors**, ensuring **secure access** to **sensitive systems and data** while enabling **interoperability** across **Member States** and **allied forces**.
   - **Benefit:** This approach **enhances security** by enabling **strong authentication** and **access control**, reduces **administrative complexity**, and facilitates **seamless collaboration** and **information sharing** among defence stakeholders across borders.

6. **Supporting Strategic Capabilities (AI, Quantum, Cyber)**

   - **Recommendation:** Ensure that the development and deployment of **advanced capabilities like AI, Quantum computing, and cyber defence tools** are underpinned by **secure, interoperable, and resilient data frameworks.**
   - **Benefit:** **Decentralised data architectures** can offer **enhanced security, control, and resilience** for sensitive data used in these critical defence domains, supporting the objectives of the Digital Europe Programme amendments.

Specific Recommendations for Action

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

- Actively promote, and where appropriate, mandate the use of the **MLETR**, the updated **eIDAS Regulation (eIDAS 2.0)**, and the **Electronic Freight Transport Information (eFTI) regulation**, not only as **foundational standards** for **commercial trade** but also as **essential layers** for **secure, interoperable data exchange** in **defence logistics**, **critical infrastructure management**, **public administration**, and **procurement**.
- Ensure the **European Digital Identity Wallet** is designed with **robust 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, equipment, and materials** within the defence supply chain and for strategic stockpiles. This would enhance **traceability from raw material to end-of-life, verify authenticity, track maintenance schedules, manage software versions, and ensure compliance** with security, safety, and ethical sourcing standards.

  For instance, a **DPP** for a **missile guidance system** could record its **raw material origins**, **manufacturing processes**, **maintenance history**, and **software updates**. This ensures **compliance with NATO interoperability standards** and enables **rapid verification** of **components** during **cross-border deployments**
- **Link DPP data with secure, interoperable platforms** to provide **real-time visibility** for logistics, maintenance, and risk assessment, contributing to the **readiness and security of supply objectives**.

3. Promote Decentralised and Resilient Architectures for Critical Defence Systems

- **Encourage and fund research, development, and deployment** of **decentralised digital infrastructures** (e.g., based on DLT, peer-to-peer networks) for critical data exchange, communication systems, command and control networks, and strategic information sharing to **enhance resilience against cyberattacks and ensure operational continuity**.

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

   - Allocate at least **15%** of the **Connecting Europe Facility (CEF) Digital's 2026–2030 budget** to **dual-use digital infrastructure investments**, such as **quantum-secure fibre optic networks** deployed along **designated military mobility routes** and **sovereign cloud nodes** strategically located near **NATO bases**. This will ensure the **physical and digital infrastructure** necessary for **secure and rapid military operations**.

   - Extend the concept of military mobility corridors to include **robust and resilient digital corridors**, ensuring **secure and uninterrupted data flow** alongside physical movement.

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

   - **Establish frameworks and dedicated funding mechanisms** (e.g., within EDF, Horizon Europe) to encourage **collaboration between public authorities** (including defence agencies and military establishments) **and the private sector** (including DigitalTrade4.EU members and other technology providers) in developing and deploying **secure, interoperable digital solutions tailored for defence applications**.

   - **Launch pilot projects** demonstrating the benefits of integrating **advanced digital trade solutions** (e.g., paperless logistics, secure e-identities, DPPs for complex equipment) with **defence supply chain management, procurement, and cybersecurity protocols**.

6. **Integrate Cybersecurity by Design into Defence Digitalisation**

   - Ensure that all digitalisation efforts within the defence sector embed **robust cybersecurity measures from the outset**, drawing from **ENISA's expertise** and aligning with the **revised Cybersecurity Act**. This includes **secure software development practices, resilient network architectures, and continuous threat monitoring** for all defence-related digital systems.

7. **Support Simplification through Digitalisation (Defence Omnibus)**

   - Recognise that the **widespread adoption of harmonised digital processes and standards** is a **powerful tool** for achieving the **simplification objectives** of the "**Defence Omnibus Simplification proposal**". **Digitalising procurement,**

certification, and cross-border administrative procedures can **significantly reduce administrative burdens** for both defence agencies and industry, **particularly SMEs**.

8. **Prioritization Framework**

   DigitalTrade4.EU recommends the Commission focus first on:

   a. **Mandating eIDAS 2.0 for defence contractor access** (short-term, high impact).

   b. **Piloting DPPs for ammunition/missile supply chains** (medium-term, addresses critical capability gaps).

   c. **Integrating MLETR into CEF military mobility corridors** (long-term, foundational interoperability).

Synergies with Green-Digital Transition for Defence

While primarily focused on environmental sustainability, the principles of the **green-digital transition** offer **relevant parallels** for the defence sector:

1. **Sustainable and Resilient Defence Supply Chains**

   The **traceability and transparency** offered by DPPs, initially for environmental data, can be adapted to ensure the **ethical sourcing of raw materials** for defence, track the **origin of components to avoid counterfeit parts**, and manage the **lifecycle of defence equipment** for better resource management and **reduced dependency**.

   This mirrors the **EU Conflict Minerals Regulation** (**Regulation (EU) 2017/821**[8]), which mandates **due diligence** for sourcing **tin, tantalum, tungsten, and gold**. Adapting similar **frameworks for defence components** would prevent reliance on **conflict-affected regions** and **counterfeit parts**

2. **Efficiency and Reduced Red Tape**

   The drive for **digitalisation in trade to reduce paper and streamline processes** (e.g., via MLETR, eFTI) directly translates to **potential efficiencies in defence procurement, logistics, and administration**, aligning with the goal of a **more agile EDTIB**.

[8] European Union. Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas https://eur-lex.europa.eu/eli/reg/2017/821/oj/eng

Conclusion and Next Steps

DigitalTrade4.EU is **firmly committed** to supporting the European Commission and Member States in achieving a **more secure, resilient, and competitive European Union**. We are convinced that the **strategic and thoughtful implementation of digital transformation, centred on interoperability, decentralisation, and harmonised standards, is not merely an auxiliary tool but a fundamental enabler** for navigating the complexities of the modern security landscape and realising the ambitions of the **European Defence Readiness 2030 strategy**.

The principles and technologies that are **revolutionising global trade and logistics** offer **profound dual-use opportunities** to enhance the EU's defence capabilities, strengthen its industrial base, and ensure its strategic autonomy. By **embracing these digital solutions**, the EU can **unlock significant synergies, improve operational efficiency, bolster security, and foster innovation** across the defence sector.

DigitalTrade4.EU proposes the following **next steps for collaboration**:

1. **Engage in a structured dialogue** with DG DEFIS, DG CNECT, EEAS, EDA, ENISA, and other relevant EU bodies to further elaborate on the practical implementation of these recommendations and explore how digital trade expertise can be leveraged for defence.
2. **Participate in relevant expert groups and consultations** concerning the implementation of the Defence White Paper, the development of the EDTIB, the Cybersecurity Act revisions, and initiatives related to dual-use technologies, bringing our consortium's expertise on digital standards, interoperability, and secure data exchange.
3. **Collaborate on pilot projects** that test and showcase the application of interoperable and decentralised digital solutions in dual-use contexts, particularly in areas such as secure defence logistics, critical component traceability using DPPs, and resilient communication networks for military mobility.

4. **Contribute to awareness-raising and capacity-building initiatives** to promote the adoption of secure and interoperable digital practices among stakeholders in the defence ecosystem, including industry (especially SMEs) and public authorities.

We are **confident** that by **working together, leveraging the expertise of both the public and private sectors**, we can build a **digital future for European defence** that is **innovative, secure, prosperous, and resilient**, ensuring the **peace and security of the Union and its citizens**.

However, challenges such as **harmonising cybersecurity protocols** across **Member States** and **mitigating risks** from **quantum computing threats** must be **proactively addressed**. Establishing a **EU-wide quantum-resistant cryptography standard** for **defence systems** could **future-proof digital infrastructure investments**. Furthermore, **continuous monitoring** and **rapid update mechanisms** should be established to respond to **evolving cyber threats**, ensuring that **digital defence infrastructure** remains **secure over time**.

We recommend the **European Cybersecurity Agency (ENISA) expedite certification of post-quantum cryptographic standards** for defence systems by Q1 2026, ensuring new digital infrastructure investments are future-proofed.

This future will be underpinned by the widespread adoption of **harmonised international digital standards** such as **UNCITRAL MLETR** and **eIDAS 2.0**, which enable **seamless interoperability**, enhance **trust**, and support both **economic competitiveness** and **defence readiness**.

EU Green-Digital Trade Leadership Roadmap (DigitalTrade4.EU, 2025)

activity	objective	indicative metrics	tools/enablers
1. EU-Singapore DTA & Expand DEPA Partnerships	Strengthen digital trade diplomacy in Asia through high-standard agreements.	- 5+ new digital trade agreements with key Asian partners (e.g., Japan, India, ASEAN) by 2030 - 15% increase in EU-Asia digital services trade by 2028	DEPA framework, EU-Singapore DTA, Global Gateway Initiative, eIDAS 2.0
2. Implement Digital Product Passports (DPPs)	Ensure traceable, sustainable supply chains aligned with EU Green Deal.	- 50% adoption of DPPs by 2030 - 20% reduction in supply-chain carbon intensity by 2030	EU Sustainable Products Initiative, CBAM incentives, UNECE Recommendation 49
3. Fund Secure Digital Corridors in Asia	Build interoperable digital infrastructure for EU-Asia trade.	- ~€2B allocated via NDICI-Global Europe - 10+ blockchain-based traceability pilots by 2027	NDICI-Global Europe, ASEAN digital customs systems, EU Customs Data Hub
4. Harmonize Digital Standards (MLETR/eIDAS 2.0)	Enable cross-border recognition of e-documents and digital identities.	- 90% mutual recognition of e-signatures by 2028 - 70% SME adoption of eIDAS wallets	MLETR framework, eIDAS 2.0, EU Transport Law updates, UN/UNECE protocols
5. Launch Green-Digital Trade Academy	Upskill SMEs and officials on DPPs and carbon accounting.	- 40% increase in SME participation by 2027 - 60% cost savings for SMEs	Erasmus+ grants, COSME programme, tiered compliance thresholds
6. Integrate ESG into Trade Finance	Link trade finance to sustainability metrics for cheaper capital access.	- €10B/year unlocked for green trade finance - 30% lower Scope 3 emissions by 2030	InvestEU guarantees, CSRD-aligned reporting, FinTech platforms
7. Enforce Platform Interoperability	Prevent vendor lock-in and empower SMEs.	- 100% compliance with CJEU rulings by 2026 - 50% reduction in platform dominance	CJEU Case C-233/23, DEPA, eIDAS 2.0, Digital Markets Act (DMA)
8. Global Digitalisation Projects with EU Standards	Extend EU digital infrastructure and norms globally.	- 20+ co-funded projects by 2030 - 80% interoperability with EU systems	Digital Europe Programme, CEF funding, EU-Asia Digital Standards Taskforce
9. Advance UNECE Transparency Protocols	Globalize EU sustainability standards for supply chains.	- 100% alignment with UNECE Rec. 49 by 2028 - 30% reduction in greenwashing claims	UNECE CEFACT, W3C Verifiable Credentials, EU CBAM registry
10. Pilot CBAM-DPP Corridors	Link trade finance to verifiable ESG metrics for tariff incentives.	- 20% CBAM compliance cost reduction - 50% DPP adoption by 2030	IoT carbon trackers, CBAM rebate schemes, EU Customs Single Window

Table 1. This roadmap outlines DigitalTrade4.EU's vision for integrating green and digital priorities into EU trade policy. While primarily focused on economic competitiveness, its principles—such as secure digital corridors and DPPs—directly support the defence sector's need for resilient supply chains and interoperable systems.