Prepared by DigitalTrade4.EU

Bolstering Cybersecurity in Ports and Maritime Trade for a Resilient Digital Europe

Feedback to the EU Commission

July 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 **108 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

1. Executive Summary

DigitalTrade4.EU emphasizes the **critical importance of cybersecurity** for the future of European Union **ports** and **maritime trade**. **Digitalisation** creates major opportunities for **efficiency** and **competitiveness**, but it also increases **vulnerability** to complex **cyber threats**. **Fragmented regulation**, skills and investment gaps, and complex **supply chains** amplify these risks, with significant **economic** and **security** implications.

A **holistic approach** to port cybersecurity—integrating **civil and defence sector** needs ("dual-use by design")—enables faster technology adoption, reduces risks, and strengthens Europe's **strategic autonomy**. **Secure and resilient ports** are directly linked to the EU's goals for **defence readiness**, the **Single Market**, and the **digital transition**.

Best practices from leading ports and countries show the value of coordinated action:

- The **Port of Rotterdam** has implemented an **integrated cybersecurity governance model** combining real-time information sharing between authorities and private operators, and regular cyber resilience exercises—leading to faster incident response and improved threat detection *(U.S. Maritime Trade and Port Cybersecurity, 2024).*
- **Singapore's Maritime and Port Authority** established a dedicated **Maritime Cybersecurity Operations Centre** and requires regular cybersecurity drills and third-party risk assessments—dramatically reducing vulnerability and improving awareness among all actors *(World Economic Forum, Global Cybersecurity Outlook 2025)*.
- The **Port of Antwerp** successfully detected and contained an insider cyberattack by investing in continuous workforce training and internal threat monitoring—demonstrating the importance of human factors and insider threat management *(Siendo, Cybersecurity Risks at Ports, 2025)*.

DigitalTrade4.EU identifies **six strategic pillars** to guide EU action:

1. **Supply chain cybersecurity** (e.g. using **Digital Product Passports**—a digital twin of physical goods tracking origin, materials, and compliance—and adopting **NIST Cybersecurity Framework (CSF) 2.0 baseline standards** for ports)

2. **Information sharing and collaboration** (e.g. **ENISA** guidelines, regional cyber exercises, trusted threat intelligence platforms)
3. **Sustainable funding models** (e.g. using **European Investment Bank** and **CEF** to co-finance cybersecurity upgrades)
4. **Resilience and workforce development** (e.g. regular manual process training, skills development programs, such as the **Union of Skills** and **Pact for Skills**)
5. **Secure integration of emerging technologies** (e.g. secure-by-design AI deployment, as practiced in Dutch and Singaporean ports)
6. **Clearer and more harmonized regulation** (e.g. aligning with **NIS2**, MLETR, and eIDAS 2.0 across Member States)

Harmonising standards, rapid **information exchange**, and targeted investment in **future-proof solutions** are key. **Cybersecurity** must be seen as a **strategic investment**, not just a compliance cost, supporting both **competitiveness** and the **Green Deal**.

DigitalTrade4.EU calls on the European Commission and Member States to **act together**: develop clear guidance and unified standards, invest in knowledge and skills, and support **pilot projects**. Only strong collaboration, learning from **international best practices**, will ensure Europe's **ports** remain **secure**, **competitive**, and resilient for the Union's long-term **security** and **economic success**.

2. Introduction

The maritime sector, with its extensive network of ports, serves as the **indispensable lifeblood of global and European Union trade**. It facilitates the movement of **over 75% of external trade and 30% of internal trade** by volume, making its efficiency and security paramount to the Union's economic stability and strategic interests. The seamless flow of goods through these critical nodes directly underpins the functioning of the Single Market and contributes significantly to Europe's global competitiveness.

Ports are currently undergoing a **rapid and profound digital transformation**, driven by the imperative to enhance efficiency and competitiveness. This involves the widespread integration of advanced Information Technology (IT), Operational Technology (OT), and Internet of Things (IoT) systems. While this interconnectedness offers substantial benefits in terms of optimized operations, improved logistics, and reduced costs, it simultaneously **expands the attack surface for malicious actors**. This heightened digital dependency renders ports **prime targets for sophisticated cyberattacks**. Recent history provides stark reminders of these tangible risks, with notable incidents crippling operations at major ports such as Antwerp, Rotterdam, Los Angeles, Barcelona, Long Beach, Houston, and the Port of Nagoya, which **suspended loading and unloading operations for two days in July 2023 due to a ransomware attack**. The longer a ship remains docked, the more vulnerable the port becomes, underscoring the continuous nature of this threat.

This dependency underscores the criticality of ports as nodes in global supply chains. For instance, disruptions at major EU ports like Rotterdam or Antwerp—which handle 15% of global container traffic—could cascade into economic losses exceeding €10 billion annually, as estimated by the European Maritime Safety Agency (EMSA) in 2024.

The evolving geopolitical landscape, characterized by escalating tensions, coupled with the increasing sophistication of cybercrime and state-sponsored Advanced Persistent Threats (APTs), poses **severe risks to critical infrastructure, including ports**. Threat actors, including nation-states like China, Russia, Iran, and North Korea, employ sophisticated techniques such as "**living off the land**" (LOTL) to persist undetected within networks for extended periods, blending their activity with normal system operations. The range of threats is broad, encompassing **ransomware, cyber-enabled fraud, supply chain attacks, and insider threats** (both negligent and malicious). The potential impacts of such attacks are far-reaching, including **severe operational disruption, significant financial losses, intellectual property theft, and, critically, human safety risks**, as attacks on critical systems can jeopardize lives. *(U.S. Maritime Trade and Port Cybersecurity, 2024; World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

Integrating Dual-Use by Design in Maritime Cybersecurity

To bolster cybersecurity in ports and maritime trade, a 'dual-use by design' model should be adopted, ensuring that R&I processes integrate civil and defence requirements from an early stage. This approach can accelerate time-to-market for technologies and eliminate barriers to technology transfer between civil and defence applications, facilitating their uptake in respective markets.

However, dual-use development carries inherent risks, including intellectual property exposure and the need to ensure confidentiality and integrity of sensitive research data. Therefore, the creation of secure and trusted R&I environments is paramount.

Key considerations for implementation include:

- **Guidance and Training:** Develop clearer guidance on dual-use obligations, including open-access requirements, for stakeholders in the maritime sector. Implement training and awareness campaigns at national and EU levels to boost compliance capacity.
- **Project Flagging:** Introduce a mechanism to identify sensitive dual-use cybersecurity projects early, enabling targeted EU support and promoting secure collaboration.
- **Export Control Compliance:** Provide tailored export control due diligence guidance, especially for SMEs, and ensure consistent dual-use or military export control checks for projects relevant to defence or security applications. Best practices from successful projects in managing export controls should be gathered and shared.

- **Ethical Governance:** Integrate mandatory ethical governance actions and initiatives into individual projects to carefully manage potential negative repercussions of dual-use research, ensuring that advancements align with societal values.

This feedback report from DigitalTrade4.EU aims to provide the European Commission with an **expert perspective on the current state of cybersecurity in EU ports and maritime trade**. It offers **actionable recommendations** designed to bolster resilience, streamline regulatory efforts, and secure the digital future of European trade, directly supporting the Union's strategic ambitions for a robust Single Market, enhanced Defence Readiness, and comprehensive Digital Transformation.

3. Expectations from the Commission's Side: The Objectives

The European Commission has articulated a **clear and ambitious strategic vision for the Union by 2030**, which inherently shapes the imperative for enhanced cybersecurity across critical sectors, including ports. This vision is characterized by a fundamental shift towards a "**defence-readiness mindset**," aiming to re-establish deterrence and enhance the collective ability of Member States and the Union's defence industry to anticipate, prevent, and respond to crises. *(Defence Readiness Omnibus, 2025)*

3.1. Overarching Strategic Vision for 2030: Defence Readiness and Civilian Infrastructure

The Commission's focus on defence readiness extends beyond purely military capabilities to encompass the **resilience of critical civilian infrastructure**. The Union's security is understood to rely on both civilian and military preparedness, with a strategic emphasis on integrating "**dual-use considerations**" into all infrastructure investments and capability planning. This includes areas such as military mobility, mass evacuations, secure communications and connectivity, maritime security, cyber capabilities, and space assets and services.

Ports, as vital components of maritime security and critical infrastructure, are therefore implicitly recognized as **integral to overall defence readiness**. A cyberattack on a major port, while not a direct military engagement, can severely cripple economic and logistical capabilities, thereby undermining the Union's broader defence posture. This understanding creates a **compelling policy imperative to invest in port cybersecurity** not merely for economic reasons, but as a core component of national and EU security and defence strategy.

3.2. Defence Readiness and Strategic Autonomy

Achieving this defence readiness requires **massive and sustained investments**, fostering a spirit of solidarity and cooperation among Member States and strategic alliances. This addresses decades of chronic under-investment and critical shortages in defence capabilities. The Commission aims to **rapidly replenish stocks and modernize armed forces**, boosting innovation cycles and simplifying research and development (R&D) procedures under the European Defence Fund (EDF). Support for start-ups and scale-ups in dual-use and defence technologies is also a priority. The Netherlands Defence Strategy for Industry and Innovation (D-SII) exemplifies this approach, explicitly listing "**Cyber and Electronic Warfare**" as one of its ten fundamental defence areas and integrating cybersecurity into key focus areas like "Intelligent Systems" and "Quantum," including ambitions for "automated detection and response to cyber attacks" and the use of "AI in cyber operations." *(Defence Readiness Omnibus, 2025; Netherlands Defence Strategy for Industry and Innovation (D-SII) 2025-2029)*

The emphasis on **dual-use technologies**, where advancements in cybersecurity for military purposes (e.g., secure communications, AI for cyber operations) can directly benefit civilian critical infrastructure like ports, and vice-versa, is particularly noteworthy. This approach provides a **strong rationale for cross-sectoral funding and collaborative R&D in cybersecurity**, effectively blurring the lines between "civilian" and "military" cybersecurity investments for critical infrastructure. *(Defence Readiness Omnibus, 2025)*

3.3. Single Market Integration and Competitiveness

The Commission views a truly functioning **EU-wide market for defense equipment** as the most effective means for Member States to re-stock their arsenals and build their readiness. Such a market is expected to **unlock economies of scale**, reduce dependence on third-country suppliers, and enhance the competitiveness of the European Defence Technological and Industrial Base (EDTIB). This principle extends to cybersecurity solutions and services. A fragmented market for cybersecurity products and services within the EU could inadvertently lead to an **over-reliance on non-EU vendors**, potentially introducing significant supply chain vulnerabilities. *(Defence Readiness Omnibus, 2025; World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

To facilitate this, the Commission proposes **substantial regulatory simplification** in defence procurement, including increasing thresholds for applicability (to EUR 900,000 for supply and service contracts), facilitating innovative procurement (e.g., new possibilities for direct procurement of innovative products from competitive research projects), extending negotiated procedures, and introducing flexible framework agreements (up to 10 years and open to other Member States). Calls have also been made to Member States to **eliminate**

"gold-plating" (imposing additional national burdens beyond EU requirements) and reduce statistical reporting obligations. Simplification of Intra-EU Transfers of Defence Products is also a key priority, with efforts to widen the use of General Transfer Licences, extend their benefit to certified companies, and simplify reporting for intangible technology transfers. Harmonized procurement and transfer rules can significantly facilitate the **widespread adoption of EU-developed secure technologies** across Member States' ports, thereby promoting a unified EU market for cybersecurity solutions. This is a strategic imperative for enhancing collective cyber resilience and reducing systemic risk from external dependencies. *(Defence Readiness Omnibus, 2025; EU Single Market Strategy, 2025)*

3.4. Digital Transformation and Innovation

Digital transformation, encompassing AI, advanced electronics, and connectivity, is deemed **critical for both the Union's competitiveness agenda and its defence resilience**. The EU's Artificial Intelligence Act promotes the development of AI systems, and Member States are encouraged to establish regulatory sandboxes for high-risk AI systems relevant for military and defense purposes, enabling legally safe development and testing.

Secure information exchange is also a cornerstone of this digital transformation. Initiatives such as the progressive rollout of the SUE (*Secret de l'Union Européenne*) system and the exploration of a Classified Cloud aim to provide secure and efficient information exchange for defence classified projects. Furthermore, the EU aims for a **paradigm shift towards a data-based Single Market**, embedding a "**digital-ready principle**" in policy design. This principle ensures that regulatory requirements are designed to be digital, interoperable, and streamlined from the outset. Key digital tools like the Digital Product Passport (DPP), EU Digital Identity Wallets, European Business Wallet, and the Once-Only Technical System (OOTS) are central to this transformation, promising to reduce administrative burdens and enable secure digital interactions. The strategy also aims to develop structured, machine-readable data formats for EU standards and digitalize public procurement procedures, embedding the "once-only principle" and introducing digital authentication. *(Defence Readiness Omnibus, 2025; EU Single Market Strategy)*

The "**digital-ready principle**", when coupled with the observed "**AI-cyber paradox**" (where rapid AI adoption often occurs without adequate security safeguards), highlights a critical need. If new digital systems and regulations are designed with cybersecurity as a foundational element from the very beginning (a "**cybersecurity by design**" approach), it can proactively prevent vulnerabilities rather than merely reacting to them. Therefore, the Commission's explicit integration of "**cybersecurity by design**" as a core component of its "digital-ready principle" for all new digital initiatives affecting critical infrastructure is essential to ensure security is foundational, not an afterthought. The Commission also addresses **long delays in standard-setting** by aiming to future-proof the standardization framework and allowing for common specifications when the system fails to deliver, connecting standardization with research and innovation efforts. *(World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report; EU Single Market Strategy)*

3.5. Cybersecurity Frameworks and Regulation

The Network and Information Security (NIS 2) Directive represents a **significant legislative act** designed to achieve a high common level of cybersecurity across the European Union, expanding its scope and strengthening requirements for critical infrastructure sectors, including maritime. Complementing this, the European Union Agency for Cybersecurity (ENISA) plays a **crucial role in formulating advice, recommendations, and guidelines** for cyber risk management in the maritime sector, aiming to enhance the resilience of critical information infrastructure and networks. *(Siendo. Cybersecurity Risks at Ports, 2025)*

While NIS 2 and ENISA provide essential frameworks and guidelines, there remains a **discernible gap between the intent of EU-level regulation and its practical implementation and harmonization** at national and local levels. Research and sectoral experience show that **regulatory fragmentation** and a **lack of standardization** can lead to poor information sharing and inadequate risk assessment in ports. This suggests that the Commission's role extends beyond issuing directives to actively supporting Member States and port operators in interpreting, harmonizing, and effectively implementing these regulations, perhaps through more prescriptive guidance or dedicated implementation support programs. Such support would be **instrumental in bridging the gap between regulatory intent and on-the-ground cybersecurity practice**. (*ENISA Threat Landscape for the Maritime Sector, 2022; Siendo. Cybersecurity Risks at Ports, 2025)*

4. Current State of Port Cybersecurity: Challenges and Vulnerabilities

Despite the strategic importance of ports and the EU's overarching objectives, the maritime sector faces a **complex array of cybersecurity challenges and vulnerabilities**. These issues, if left unaddressed, pose significant risks to the continuity of trade, economic stability, and national security.

4.1. Supply Chain Vulnerabilities

One of the most critical challenges is the **pervasive lack of cyber supply chain visibility** and the absence of standardized Cyber Supply Chain Risk Management (C-SCRM) practices. Port cybersecurity actors frequently lack comprehensive knowledge of vulnerabilities within their extended software supply chain, extending to third-party and even Nth-party providers. This limited visibility, coupled with a proliferation of differing SCRM frameworks, means that port actors rarely share a common language for discussing risk, hindering holistic risk assessments. The increasing complexity of supply chains and a lack of oversight into supplier security levels are major issues, with **supply chain challenges identified as the top ecosystem cyber risk by 54% of large organizations**, indicating widespread vulnerability across industries and sectors (World Economic Forum, 2025). This high tolerance for low levels of assurance means that vulnerabilities introduced by third parties can propagate cyberattacks throughout the entire ecosystem. Concerns also persist regarding the storage and maintenance of sensitive data abroad or in inaccessible locations, making it more susceptible to tampering or collection. Furthermore, while compromises to OT systems are prioritized for security, there are significant challenges in understanding the full effect of a compromise on port operations, and many actors have unknown or little visibility into their downstream providers and minimal awareness of the components or contributors supporting the software they use. *(U.S. Maritime Trade and Port Cybersecurity, 2024; World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

4.2. Operational and Information Gaps

A significant impediment to effective cybersecurity in ports is the **pervasive lack of coordination and inconsistent communication** among various stakeholders, both before and during crises. Post-incident reviews consistently highlight coordination and communication as areas requiring substantial improvement. Information sharing often relies on informal networks within the private sector, rather than established government-to-private mechanisms, which can be slow and inefficient. A culture of self-preservation and competition among businesses in the maritime transportation system can lead to **information hoarding**, further impeding formal collaboration and rapid dissemination of critical threat data. *(U.S. Maritime Trade and Port Cybersecurity, 2024)*

4.3. Specific Threat Vectors

Ports are exposed to a range of sophisticated and impactful cyber threats:

- **Ransomware:** This remains a **primary concern**, often spread through phishing emails, capable of crippling affected systems. The July 2023 attack on the Port of Nagoya, which suspended operations for two days , and the NotPetya malware's significant financial losses for Maersk, underscore the devastating impact of ransomware *(U.S. Maritime Trade and Port Cybersecurity, 2024)*.
- **Insider Threat:** Whether negligent or malicious, insider threats exploit trusted access to infrastructure. Negligent insiders may be careless or fail to follow security policies, while malicious insiders, sometimes collaborating with external actors (as seen in the Port of Antwerp attack), can cause prolonged undetected damage due to a lack of formal policies and training.
- **Advanced Persistent Threats (APTs):** Nation-states frequently sponsor APT activities targeting critical infrastructure. These actors use sophisticated techniques, such as "**living off the land**" (LOTL), to persist undetected within networks for extended periods, blending their activity with normal system operations. Volt Typhoon is a recent APT concern that could affect virtually all critical infrastructure, including ports.
- **Non-Cyber Attack Vectors (Shell Companies):** Shell companies can obscure true ownership, allowing threat actors to evade sanctions and gain access to restricted

physical or digital areas of ports to stage further attacks, or for criminal activities and state-backed espionage.

4.4. Economic and Financial Barriers

The **financial landscape** for **port cybersecurity** in the **European Union** is marked by **fragmentation**, **lack of transparency**, and persistent **underinvestment**. The **cyber insurance market** remains **complex and confusing** for port operators, with significant variation in coverage, requirements, and exclusions across Member States *(ENISA Threat Landscape for the Maritime Sector, 2022).* Many **insurance policies** fail to cover **systemic or nation-state cyberattacks**, leaving ports exposed to potentially severe losses and not incentivising sufficient investment in **robust cyber defences** *(World Economic Forum, 2025).*

Funding for port cybersecurity is often **short-term and project-based**, leading to **reactive spending** and a focus on **compliance** rather than on **strategic risk management** (**European Maritime Safety Agency, 2024**). Many port operators lack reliable methods to assess the **economic impact** of cyber incidents or to calculate the **return on investment** in cybersecurity measures. As a result, **cybersecurity** is still too often seen as a **cost of compliance**, not as a **strategic investment** for resilience and competitiveness, and cybersecurity experts are rarely involved in executive-level budget planning.

The **European Commission** should ensure that **EU funding programmes** for port cybersecurity are **well-resourced, long-term, and strategically targeted**. Innovative models—such as **EU-level public-private investment platforms** and **harmonised cyber insurance standards**—are needed to support greater **resilience** and **competitiveness** in the digital trade environment.

4.5. Resilience Deficiencies

The ability of ports to **revert to manual processes and maintain operations in a degraded state** following a disruptive cyberattack is questionable and largely untested. Surveyed ports do not regularly exercise for the transition from digital to manual cargo processing, which would inevitably cause delays due to training needs. Even with a fully trained workforce, throughput would be significantly reduced (up to 90% degradation), and labor costs would increase. A critical concern is the **aging workforce** with experience in non-digitized operations; their knowledge of historical manual processes has not been adequately recorded for younger employees, creating a **two-factor risk**: the loss of knowledge and a potential "labor shortage" if younger cohorts are not trained. This encourages a "**fix it**" mentality rather than proactive preparation for continued operations in a degraded state. *(U.S. Maritime Trade and Port Cybersecurity, 2024; World Economic Forum. (2025). Global Cybersecurity Outlook, 2025)*

4.6. Impact of Digitalization

While digitalization offers many conveniences, it introduces **new dangers**. The increasing interconnectedness of ships and maritime infrastructure heightens the potential for successful cyberattacks. Modern ports' reliance on numerous integrated IT, OT, and IoT platforms, many of which still depend on **legacy technologies and systems not designed for stringent cybersecurity requirements**, creates significant vulnerabilities. A successful attack can lead to loss of confidentiality, integrity, or availability of data, ultimately causing substantial harm to business operations. *(Siendo. Cybersecurity Risks at Ports, 2025; European Maritime Safety Agency (EMSA), 2023; Global Cybersecurity Outlook, 2025)*

4.7. Regulatory Complexity

Confusing regulations and a lack of standardization significantly impact cybersecurity in ports by creating challenges in information sharing, hindering effective risk management, and complicating incident response. Post-incident reviews frequently identify coordination and communication as areas needing improvement, exacerbated by confusing federal laws and regulations regarding reporting. For example, in some countries (such as the United States), overlapping requirements between federal and state legislation create confusion and inconsistent notification procedures. In the **European Union**, similar complexity may arise when national “gold-plating” adds layers to **EU-level directives** such as **NIS2**. **Simplifying and harmonising the EU regulatory framework** remains essential to effective incident response and communication between public and private actors. *(ENISA Threat Landscape for the Maritime Sector, 2022)*

A proliferation of Supply Chain Risk Management (SCRM) frameworks means that actors in the port ecosystem rarely share a common language for discussing risk. This **lack of standardization**, coupled with limited visibility into cyber and software supply chains, leaves ports largely unable to develop holistic risk assessments. The global proliferation and fragmentation of regulatory requirements also add significant compliance burdens, leading to "**regulatory fatigue**" and potentially detracting from the development of customized, risk-based strategies. *(U.S. Maritime Trade and Port Cybersecurity, 2024; World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

4.8. Broader Ecosystem Challenges

The maritime sector also contends with broader cybersecurity ecosystem challenges. The **widening cyber skills gap** has increased, with two out of three organizations reporting moderate-to-critical skills gaps, making it challenging to manage cyber risks effectively. Additionally, the "**AI-cyber paradox**" presents a significant concern: while 66% of organizations expect AI to significantly impact cybersecurity, only 37% have processes to assess the security of AI tools before deployment. This rapid adoption without necessary security safeguards creates new vulnerabilities, as cybercriminals are increasingly leveraging Generative AI (GenAI) to augment their capabilities, making attacks more sophisticated and scalable and lowering the barriers to entry for cybercrime. This issue is particularly alarming for smaller organizations, with 69% lacking adequate safeguards, exacerbating **cyber inequity** and increasing the collective vulnerability of the entire ecosystem. *(World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

4.9. Enhancing Cross-Border Coordination and EU-Level Harmonization

A persistent challenge in European port cybersecurity is the fragmented approach to both risk management and regulatory implementation across Member States. While many cybersecurity threats are transnational by nature—such as ransomware campaigns or supply chain attacks—responses often remain limited to national frameworks, leading to duplication of efforts and vulnerability gaps at borders.

To address these cross-border risks, it is essential to strengthen EU-level coordination and promote a unified approach to risk assessment, incident response, and regulatory compliance. This includes:

- **Conducting regular, EU-wide cyber incident response exercises involving multiple Member States and cross-border port operators** to ensure operational readiness in case of large-scale attacks.
- **Developing and implementing joint risk assessments at the EU level**, allowing ports and authorities to benefit from shared threat intelligence and best practices, and to identify systemic vulnerabilities that may not be apparent at the national level.
- **Establishing clear, EU-wide protocols for notification and information sharing** during cyber incidents, particularly those with potential cross-border or Single Market impact, to enable rapid and harmonized responses.
- **Actively supporting the harmonization and mutual recognition of cybersecurity standards and certification schemes** (such as those developed under NIS2 and ENISA) across all EU ports to avoid regulatory fragmentation and reduce the compliance burden for operators involved in cross-border trade.
- **Encouraging Member States to minimize 'gold-plating'**—the practice of adding extra national requirements (e.g., redundant certifications or reporting formats) on top of EU legislation—which creates additional complexity and hinders the effectiveness of a single, integrated European cybersecurity market.

Ultimately, **cybersecurity for European ports must be recognized as a shared European responsibility, requiring integrated risk management frameworks and seamless regulatory cooperation across borders**. Failure to achieve this can result in critical vulnerabilities that compromise not only individual ports, but the security and resilience of the entire European trade network.

5. Approach and Recommendations

To address the multifaceted cybersecurity challenges confronting EU ports and maritime trade, DigitalTrade4.EU proposes a **comprehensive, multi-pronged approach** grounded in strategic imperatives and leveraging existing and proposed EU initiatives. The aim is to foster a truly resilient and secure digital trade ecosystem that aligns with the Commission's broader objectives for defence readiness, single market integration, and digital transformation.

The Port of Rotterdam has implemented an integrated cybersecurity governance model combining real-time information sharing between public authorities and private stakeholders. Regular cyber resilience exercises, mandatory supply chain risk management policies, and strong collaboration with the Dutch National Cyber Security Centre have demonstrably reduced incident response times and improved threat detection.

5.1. Core Principles for Digital Trade Resilience

DigitalTrade4.EU advocates for an approach grounded in three core principles to foster a secure and efficient digital trade ecosystem:

1. **Global Interoperability:** Ensuring that digital systems and data can be seamlessly exchanged and understood across different countries and platforms.
2. **Decentralisation:** Fostering an environment that supports technologically neutral, decentralized, and resilient architectures, such as those based on Distributed Ledger Technology (DLT) or peer-to-peer networks, rather than mandating a single, centralized system. This enhances security by eliminating single points of failure, increases resilience against cyberattacks, and gives economic operators greater control over their data.
3. **Adoption of Harmonised International Digital Legal Frameworks and Standards:** Championing the use of globally recognized legal frameworks like the **UNCITRAL**

Model Law on Electronic Transferable Records (MLETR)[1] and the **Regulation (EU) 2024/1183 (eIDAS 2.0)**[2].

5.2. Strategic Imperatives for Digital Trade Resilience

5.2.1. Holistic Cyber Supply Chain Management

Given that supply chain vulnerabilities represent a top ecosystem cyber risk, a **robust and standardized approach to Cyber Supply Chain Risk Management (C-SCRM) is paramount**.

- **Establish and Enforce Minimum Visibility Standards:** The Commission should explore incentives, such as subsidies, to encourage firms in critical infrastructure to **maintain basic standards of visibility** over their immediate software suppliers and throughout their extended supply chains. This includes requiring firms to understand the cybersecurity posture of their direct software providers and to enforce security standards on third-party and Nth-party providers. Information on software supply chains and vulnerabilities should also be shared at the regional level. *(U.S. Maritime Trade and Port Cybersecurity, 2024; World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*
- **Standardize Cybersecurity Supply Chain Risk Management (C-SCRM) Frameworks:** A **common language and approach to discussing risk** across the entire port ecosystem are urgently needed. The Commission should work towards standardizing C-SCRM frameworks across industry and port actors to improve understanding and coordination. DigitalTrade4.EU recommends **adopting the NIST Cybersecurity Framework (CSF) 2.0 as a baseline** for EU ports due to its integration of supply chain risk management and alignment with ISO/IEC 27001, ensuring compatibility with existing EU cybersecurity certifications
- **Develop Model Contractual Language:** To mitigate risks introduced by external suppliers, the Commission should **draft and disseminate examples of robust**

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

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

contractual language for ports to use with third-party vendors, ensuring clear cybersecurity obligations and accountability.

- **Promote Standardization and Certification:** Standardization and certification mechanisms should be promoted to **increase trust in services** provided within the digital ecosystem, particularly for critical components and services. Organizations should also reconsider risk exposure throughout their entire end-to-end supply chain and enforce secure software development practices, including robust risk assessment and dependency management. *(World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

- **Digital Product Passports (DPPs) and Extend for Dual-Use:** DigitalTrade4.EU fully supports the EU's vision for DPPs as a fundamental enabler of supply chain transparency and sustainability. Furthermore, DigitalTrade4.EU recommends **extending the DPP framework beyond commercial applications to cover critical components, equipment, and materials within the defence supply chain**. This would enable real-time tracking of military assets, combat counterfeiting, and ensure compliance with stringent security and ethical sourcing standards, directly supporting European defence objectives.

- **Fostering Supply Chain Security and Transparency through Globally Unique Identifiers:** The eFTI framework, under Regulation (EU) 2020/1056 on Electronic Freight Transport Information (eFTI) can be significantly strengthened by integrating a mechanism for verifying the legal and operational status of economic operators. This is achievable by **mandating the use of a globally recognized legal entity identifier, specifically the Legal Entity Identifier (LEI)**, for every economic operator involved in a transaction. DigitalTrade4.EU recommends integrating LEI and its verifiable counterpart (vLEI) into the eFTI and DPP frameworks to ensure reliable identification of all legal entities, reduce fragmentation, improve regulatory compliance, and bridge EU and third-country identifiers for cross-border interoperability.

5.2.2. Enhanced Information Sharing and Collaborative Response

Effective incident management and threat mitigation are impossible without timely and comprehensive information sharing.

- **Formalize Information Sharing Architectures:** Encourage and support the use of existing regional information sharing structures, while simultaneously working to build enhanced, **formalized processes that bridge the public and private sectors**. This includes establishing robust information sharing architectures that facilitate real-time, threat-based information exchange between public authorities and private sector stakeholders, in line with the requirements of the **NIS2 Directive**, guidance from the **European Union Agency for Cybersecurity (ENISA)**, and relevant national reporting obligations.
- **Clarify Reporting Procedures:** Once final rules for cyber incident reporting are published, relevant authorities must conduct extensive outreach to **clarify expectations, deconflict or eliminate ineffective communication patterns, and harmonize information sharing** throughout the cyber incident management process.
- **Increase Multi-Stakeholder Cyber Incident Management Exercises:** Regular exercises involving all stakeholders are crucial to **identify vulnerabilities, address communication issues, and build stronger collaboration** among all parties involved in cyber incident response.
- **Provide Robust Threat Data:** Government entities should provide **more detailed, robust threat data** to private sector actors, enabling them to better prepare and defend against attacks. Furthermore, fostering private-to-private information-sharing mechanisms at regional and national levels can **expedite the dissemination of urgent threat information** more rapidly than government-to-private channels alone.
- **Interlinking Digital Compliance Portals and Platforms:** The European Commission should prioritize the **seamless interoperability of various digital compliance portals and platforms**, including Maritime Single Window, eFTI, DPP, and sector-specific portals. This interoperability is critical to avoid data duplication, reduce administrative

burdens, and streamline regulatory reporting and enforcement across Member States, creating a more efficient, cost-effective, and secure digital environment.

5.2.3. Sustainable Investment and Funding Models

Addressing the chronic underinvestment in port cybersecurity requires a fundamental shift in funding mechanisms and a change in perception of cybersecurity as a cost centre. *(European Maritime Safety Agency (EMSA), Annual Report 2024)*

- **Expand and Enhance Dedicated Funding Programs:** The bottleneck for maritime cybersecurity funding, often reliant on temporary stop-gap programs, must be eliminated by **expanding and enhancing dedicated programs**. This should include increasing funding levels to meet actual needs (estimated at significantly more than current allocations) and incorporating more stringent cybersecurity requirements into program guidelines. The **European Commission** should ensure that **EU funding programmes** for **port cybersecurity** are adequately **resourced**, **easy to access**, and focused on driving **measurable improvements** in **cyber resilience** across all **European ports**.
- **Integrate Cybersecurity into Executive Decision-Making:** Port executive leaders must view cybersecurity as an **executive priority** and invest in forward-leaning, enterprise-wide cybersecurity strategies. Chief Information Officers (CIOs) should be integral to planning for grant submissions and overall budget discussions to ensure requests align with actual cybersecurity needs and strategic investments.
- **Promote Cybersecurity as a Competitive Differentiator:** Firms should be encouraged to adjust their perspective on cybersecurity, highlighting **enhanced security standards as a competitive selling point** to clients. This proactive approach views cybersecurity investment as a business advantage rather than merely a compliance cost.

5.2.4. Proactive Resilience Planning and Workforce Empowerment

True resilience extends beyond preventing attacks to ensuring continued operations in degraded states and fostering a skilled workforce capable of adapting to evolving threats.

- **Integrate Training for Manual Procedures:** Contingency plans for resilient port operations must **integrate regular training for manual procedures**, ensuring the capacity to move critical goods even if digital systems are compromised. Facilities should regularly exercise business continuity management and resilience operations, including non-digitized operations, and certify their ability to operate without IT and, to the greatest extent possible, OT systems for short periods. *(U.S. Maritime Trade and Port Cybersecurity, 2024)*

- **Address Knowledge Transfer and Skills Gap:** Funding programs should specifically focus on **training for recovery and resilience**, as well as updating cyber infrastructure. Strategies are needed to capture and transfer the knowledge of aging workforces experienced in non-digitized operations to younger employees, mitigating the risk of knowledge loss and potential labor shortages during a manual reversion. Organizations should also look beyond traditional cyber qualifications to recruit talent from non-traditional backgrounds and utilize strategic cybersecurity talent frameworks. *(U.S. Maritime Trade and Port Cybersecurity, 2024; World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

- **Develop AI Competencies and Prioritize Workforce Well-being:** Organizations must commit to equipping their workforce with necessary AI competencies and continually updating educational curricula to mirror the dynamic cyberthreat landscape. Prioritizing workforce well-being and retention is also crucial to address burnout in the cybersecurity sector. *(World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

- **Balance Automation with Manual Planning:** While maintaining a competitive edge will require additional digitization and automation, the enhancement in automated processes should not detract from contingent, manual operations planning and training to ensure resiliency. *(U.S. Maritime Trade and Port Cybersecurity, 2024)*

- **Invest in Business Resilience Strategies:** Companies must invest in their own business resilience strategies, ensuring they have contingency plans that do not rely solely on their SaaS partners, as no system is infallible. *(World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

5.2.5. Secure Integration of Emerging Technologies

The rapid adoption of emerging technologies, particularly AI, necessitates a "**security-by-design**" approach to prevent the introduction of new vulnerabilities.

- **Implement Cybersecurity by Design for AI:** Organizations must implement strategies and processes for **secure AI implementation from the outset**, assessing the security of AI tools prior to deployment. This includes inventorying all new assets relating to AI infrastructure, securing training data, and continuously monitoring AI system behaviour to detect manipulation. Building a strong cyber culture is central to integrating AI safely into an organization, requiring a holistic approach to secure AI adoption. *(World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

- **Leverage AI for Cyber Defence:** AI offers immense opportunities to **augment human abilities in cyber defence**, making it stronger and more efficient through automated detection and response, processing vast amounts of data for early threat detection, and enhancing threat alert triage. The Commission should support initiatives that explore AI for cyber operations and cybersecurity. *(Netherlands Defence Strategy for Industry and Innovation (D-SII) 2025-2029; World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

- **Proactive Risk Assessments for New Technologies:** Comprehensive risk assessments for all new technologies, including quantum computing, must be conducted to understand and mitigate potential threats before widespread deployment. *(World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

- **Invest in Dual-Use Digital Infrastructure:** Allocating a significant portion of the Connecting Europe Facility (CEF) Digital budget to **dual-use digital infrastructure, such as quantum-secure networks along military mobility corridors**. This ensures that physical and digital infrastructure are co-developed to support secure and rapid military and commercial operations, while also developing robust EU digital infrastructure.

5.2.6. Streamlining the Regulatory Landscape

The current proliferation and fragmentation of regulatory requirements create significant compliance burdens and can detract from effective cybersecurity strategies.

- **Advocate for Global Regulatory Harmonization:** Public-private cooperation is urgently needed to enable **global regulatory harmonization and alignment**, ensuring consistency in cybersecurity standards across diverse regions while allowing for flexibility to adapt to emerging threats. *(World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

- **Targeted EU-Level Simplifications:** The Commission's efforts to simplify regulations, such as increasing thresholds for defence procurement, streamlining EDF procedures, and clarifying the application of non-defence-specific EU legislation (e.g., REACH, AI Act) to defence needs, should be **consistently applied and extended to critical civilian infrastructure like ports** where relevant. This includes simplifying permitting processes for defence industrial investments and activities, clarifying existing derogations in environmental legislation, and addressing defence readiness needs in chemicals acquis. *(Defence Readiness Omnibus, 2025)*

- **Address "Gold-plating":** Member States should be strongly encouraged to **review and remove additional national burdens** ("gold-plating") on participants in procurement and transfer procedures, which hinder efficiency and cross-border cooperation. *(Defence Readiness Omnibus, 2025)*

- **Consistent Application of "Digital-Ready Principle":** The "**digital-ready principle**" should explicitly incorporate "**cybersecurity by design**" for all new digital initiatives affecting critical infrastructure, ensuring that security is a foundational element from the outset. *(EU Single Market Strategy, 2025; World Economic Forum. (2025). Global Cybersecurity Outlook 2025: Insight Report)*

- **Champion EU-wide Adoption of the MLETR Legal Framework:** DigitalTrade4.EU strongly recommends that the Commission **champion the adoption of the UNCITRAL MLETR legal framework** across all Member States. This model law provides a globally recognized legal basis for electronic transferable records to be treated as functionally equivalent to their paper counterparts, which is an essential first step towards a legally certain, paperless, and efficient trade environment aligned with global trading partners.

- **Leverage eIDAS 2.0 for a Secure and User-Controlled Digital Identity:** The European Digital Identity (EUDI) Wallet, established under the new eIDAS 2.0 Regulation, should serve as the cornerstone of trusted digital identity in the EU, complemented by the EU Business Wallet. These frameworks empower citizens and businesses by granting them full control over their data, allowing secure storage and sharing of identity information and verifiable credentials across borders. Compatibility with international unique identity (UID) systems like the Legal Entity Identifier (LEI) should also be prioritized to align with global standards.

5.3. Leveraging EU Initiatives for Port Cybersecurity

The EU has numerous existing and proposed initiatives that can be **strategically leveraged to bolster port cybersecurity** and digital trade infrastructure.

- **European Defence Fund (EDF) and Related Programs:** The EDF, designed for knowledge development, innovation, and industrialization of R&D, should explicitly **prioritize projects that have dual-use applications for critical civilian infrastructure cybersecurity**, particularly in areas like secure communications, AI for cyber operations, and quantum resilience. Simplifications introduced to the EDF, such as clarified and simplified award criteria, flexible work programmes, and broader possibilities for indirect management, should be utilized to fast-track relevant cybersecurity projects. *(Defence Readiness Omnibus, 2025; Netherlands Defence Strategy for Industry and Innovation (D-SII) 2025-2029)*
- **Investment and Funding Instruments:** Instruments like the European Investment Bank (EIB), European Investment Fund (EIF), and InvestEU Fund should **adapt their eligibility criteria to better facilitate access to financing** for port cybersecurity initiatives, recognizing their contribution to both economic resilience and defence readiness. The Strategic Technologies for Europe Platform (STEP) and the European Innovation Council (EIC) Accelerator should actively open to dual-use and defence

technologies that can enhance port security. The Netherlands' "Defport" initiative, with its Financing Table, serves as a valuable model for strengthening dialogue between government, financiers, and the Defence industry, and increasing awareness of national and EU investment funds and opportunities. *(Defence Readiness Omnibus, 2025, 2025; Netherlands Defence Strategy for Industry and Innovation (D-SII) 2025-2029)*

Expanding the Defport model to EU ports could involve establishing a 'Cybersecurity Investment Platform' under the European Investment Bank (EIB). This platform would pool public and private funds to co-finance port cybersecurity upgrades, mirroring the EIB's role in the €1.5 billion Clean Maritime Demonstration Fund launched in 2023.

- **Cybersecurity Agencies and Directives:** ENISA's guidelines for cyber risk management in ports should be **widely promoted and actively supported** through capacity building and training programs for port operators. The NIS 2 Directive's expanded scope and strengthened requirements for critical infrastructure must be **rigorously implemented across all Member States**, with the Commission providing clear guidance to harmonize its application and reporting procedures. *(Siendo. Cybersecurity Risks at Ports, 2025)*
- **Digital Single Market Tools:** The rollout of EU Digital Identity Wallets, the European Business Wallet, and the Once-Only Technical System (OOTS) can significantly **reduce administrative burdens and enhance secure digital interactions** within the maritime logistics chain, contributing to overall cyber resilience. The Digital Product Passport (DPP) can streamline compliance and provide crucial information for supply chain security. Other tools like the EU Company Certificate, Business Registers, and eInvoicing can further digitalize the single market. *(EU Single Market Strategy)*
- **Skills Development Programs:** Initiatives under the "**Union of Skills**," including the STEM Education Strategic Plan and the Pact for Skills, should be specifically tailored to **address the cyber skills gap in the maritime sector**, supporting vocational excellence centers and workforce mobility programs dedicated to cybersecurity. *(Defence Readiness Omnibus, 2025; Netherlands Defence Strategy for Industry and Innovation (D-SII) 2025-2029)*

- **Broader Defence Industry Initiatives:** Efforts to achieve **increased European strategic autonomy in security and Defence**, scale up production capacity of military equipment, and encourage **joint procurement and joint R&D** are all relevant. The Netherlands' commitment to **convergence of arms export policies** and advocating for **open supply chains** among European OEMs also contributes to a more resilient and integrated European defence industrial base, which indirectly benefits critical civilian infrastructure. *(Netherlands Defence Strategy for Industry and Innovation (D-SII) 2025-2029)*

6. Conclusion and Next Steps

The **security** and **resilience** of European **ports** and **maritime trade** are crucial for the European Union's **prosperity**, **strategic autonomy**, and ability to respond to evolving global threats. The accelerating **digitalisation** of the sector increases both opportunity and **vulnerability**, making **coordinated, proactive action** essential.

To build a truly **secure and resilient port ecosystem**, the EU must move beyond fragmented approaches and embrace a **unified, forward-looking strategy** grounded in the following priorities:

- **Establish strong governance** at EU level, with a dedicated working group to coordinate cybersecurity efforts and align Member States on key standards and regulations.
- **Launch targeted pilot projects** to accelerate the adoption of integrated cybersecurity solutions and foster effective information sharing between public and private stakeholders.
- **Harmonise regulations and standards**—notably for NIS2, eIDAS 2.0, and supply chain risk management—ensuring clarity and reducing compliance complexity across the Single Market.
- **Secure sustainable funding** for cybersecurity investments, using EU instruments and encouraging public-private partnerships to deliver long-term impact.
- **Prioritise workforce development** by investing in both digital skills and operational resilience, ensuring ports can respond to and recover from cyber incidents.
- **Support the secure integration of emerging technologies** by embedding "security by design" and conducting regular risk assessments.

Cybersecurity in ports must be seen as a **strategic investment** that underpins not only the efficiency of trade but also Europe's broader **security**, **sustainability**, and **economic competitiveness**.

DigitalTrade4.EU calls on the European Commission and Member States to **act decisively and collaboratively**—adopting clear guidance, removing barriers to investment and innovation, and building the capacity needed to safeguard Europe's position as a global leader in digital and sustainable trade.

DigitalTrade4.EU stands ready to partner in this effort and to support the implementation of these recommendations, ensuring that Europe's ports remain secure, resilient, and future-ready.

Appendix 1. Top 5 Cybersecurity Risks for European Ports (2025)

#	Risk Category	Description	Potential Impact	Example
1	**Ransomware Attacks**	Malicious software encrypts systems, demanding ransom for recovery.	Operational shutdown, financial loss, reputational damage	Port of Nagoya, Maersk (NotPetya)
2	**Supply Chain Vulnerabilities**	Lack of visibility and control over third-party and Nth-party risks in software/hardware supply chain.	Attack propagation, ecosystem disruption, compliance gaps	SolarWinds, Log4j vulnerabilities
3	**Insider Threats**	Negligent or malicious insiders abusing trusted access.	Data theft, sabotage, undetected system compromise	Port of Antwerp (insider breach)
4	**Advanced Persistent Threats (APTs)**	Nation-state actors employ stealthy, long-term attacks on critical systems.	Espionage, disruption, undetected data exfiltration	Volt Typhoon, state-sponsored APTs
5	**Regulatory Complexity & Information Gaps**	Fragmented and overlapping regulations hinder effective response and information sharing.	Delayed response, non-compliance, regulatory fatigue	Overlapping NIS2, national rules
6	**Phishing and Social Engineering**	Deceptive tactics to trick employees into revealing sensitive data or system credentials.	Unauthorized access, credential theft, network compromise	Targeted phishing emails to port staff
7	**Legacy Systems & Outdated Technology**	Continued use of unsupported or insecure systems vulnerable to exploitation.	System compromise, increased attack surface, costly downtime	OT/IT legacy equipment in older terminals
8	**Insufficient Cybersecurity Funding**	Underinvestment in cyber defenses, insurance, and training.	Gaps in preparedness, slow recovery, persistent vulnerabilities	Low cyber insurance uptake, budget cuts
9	**Lack of Skilled Cybersecurity Workforce**	Difficulty in attracting and retaining qualified cyber talent.	Inadequate monitoring, delayed detection, slow incident response	Cyber skills gap in maritime sector
10	**IoT/IIoT Device Vulnerabilities**	Poorly secured Internet of Things and Industrial IoT devices in port operations.	Remote takeover, disruption of critical systems, data leakage	Exploited IoT sensors/controls in ports

Table 1: The top ten cybersecurity risks currently facing European ports, based on analysis of recent incidents, international reports, and sectoral studies. These risks reflect the most common, impactful, and persistent threats identified in both industry practice and regulatory assessments. Note: The ranking is based on a combined assessment of risk frequency in leading sector reports, recent high-profile incidents, and the potential business and economic impact, rather than solely on the number of occurrences or monetary loss. Main sources for this overview include U.S. Maritime Trade and Port Cybersecurity (2024); the World Economic Forum Global Cybersecurity Outlook 2025: Insight Report; Siendo's Cybersecurity Risks at Ports (2025); and European Maritime Safety Agency (EMSA) reports.

Appendix 2. Best Practices in Port Cybersecurity (2025)

Best Practice	Description	Example/Outcome
Multi-Stakeholder Cyber Exercises	Regular cyber drills involving public authorities, private operators, and supply chain partners.	Improved crisis response and faster recovery (e.g. Port of Rotterdam).
Real-Time Threat Intelligence Sharing	Active participation in trusted information sharing networks at regional, national, and EU level.	Earlier detection and response to new threats.
Adoption of International Cybersecurity Standards	Implementation of standards such as NIST CSF 2.0 and ISO/IEC 27001 as a baseline for risk management.	Consistent protection and easier compliance across ports.
Comprehensive Supply Chain Risk Management	Mapping, monitoring, and auditing third-party and Nth-party suppliers for cyber risks.	Reduced supply chain vulnerabilities, better contract clauses.
Investment in Workforce Training & Awareness	Regular training for all staff, from executives to front-line workers, including simulated phishing tests.	Fewer successful attacks due to human error; higher cyber resilience.
Cybersecurity by Design for Emerging Technologies	Secure-by-design approach for new IT, OT, and AI deployments, including secure onboarding of IoT devices.	Fewer exploitable vulnerabilities in digital transformation projects.
Backup and Recovery Drills	Routine testing of backup systems and manual procedures for critical functions.	Shorter downtime, maintained operations during incidents.
Harmonized Incident Reporting Protocols	Use of standardized, EU-level reporting and escalation processes for cyber incidents.	Faster, more coordinated cross-border response.
Participation in EU Cyber Capacity-Building Initiatives	Involvement in ENISA, NIS2, and sectoral skills programs.	Access to latest knowledge, funding, and best practices.
Continuous Monitoring and Vulnerability Management	24/7 system monitoring, regular vulnerability scanning, and rapid patch management.	Early identification and mitigation of threats.
AI/ML-based Threat Detection and Anomaly Monitoring	Use of artificial intelligence and machine learning to detect abnormal patterns and suspicious activity in real time.	Early detection of novel attacks, faster response to zero-day threats.
Pattern Recognition for Proactive Defense	Implementation of advanced analytics to identify repeating attack patterns or behaviors across port networks.	Prevention of recurring incidents and improved situational awareness through real-time anomaly detection.

Table 2: Leading cybersecurity best practices for European ports, compiled from international case studies, regulatory guidelines, and DigitalTrade4.EU recommendations. The listed practices have demonstrably improved cyber resilience and response capabilities in the maritime sector.

Appendix 3. 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, prioritizing cybersecurity resilience	- ~€2B allocated via NDICI-Global Europe - 10+ blockchain-based traceability pilots by 2027	NDICI-Global Europe, ASEAN digital customs systems, EU Customs Data Hub, ENISA threat intelligence platforms
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	Implement LEI and vLEI for Supply Chain Trust	Harmonise and simplify legal entity identification across borders	- 90% entity coverage with LEI by 2030; 50% vLEI use in customs and eFTI transactions	ISO 17442, vLEI, eIDAS 2.0, UNECE UID
6	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
7	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
8	Enforce Platform Interoperability	Prevent vendor lock-in and empower SMEs.	- 100% compliance with CJEU rulings by 2026 - 50% reduction in platform dominance	Court of Justice of the European Union (CJEU) Case C-233/23, DEPA, eIDAS 2.0, Digital Markets Act (DMA)
9	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
10	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
11	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 4. The roadmap above, DigitalTrade4.EU's input to the European Commission's "International Digital Strategy" operationalises the recommendations outlined in this document. For instance, Activity 1 (EU-Singapore DTA & Expand DEPA Partnerships) directly supports the harmonisation of international digital standards, while Activity 8 (Global Digitalisation Projects with EU Standards) aligns with efforts to promote dual-use infrastructure globally, particularly by integrating robust cybersecurity measures designed to serve both civilian maritime operations and defence needs, ensuring strategic autonomy and resilience. These activities collectively reinforce the EU's ability to leverage digital trade diplomacy as a tool for both economic growth and strategic security.